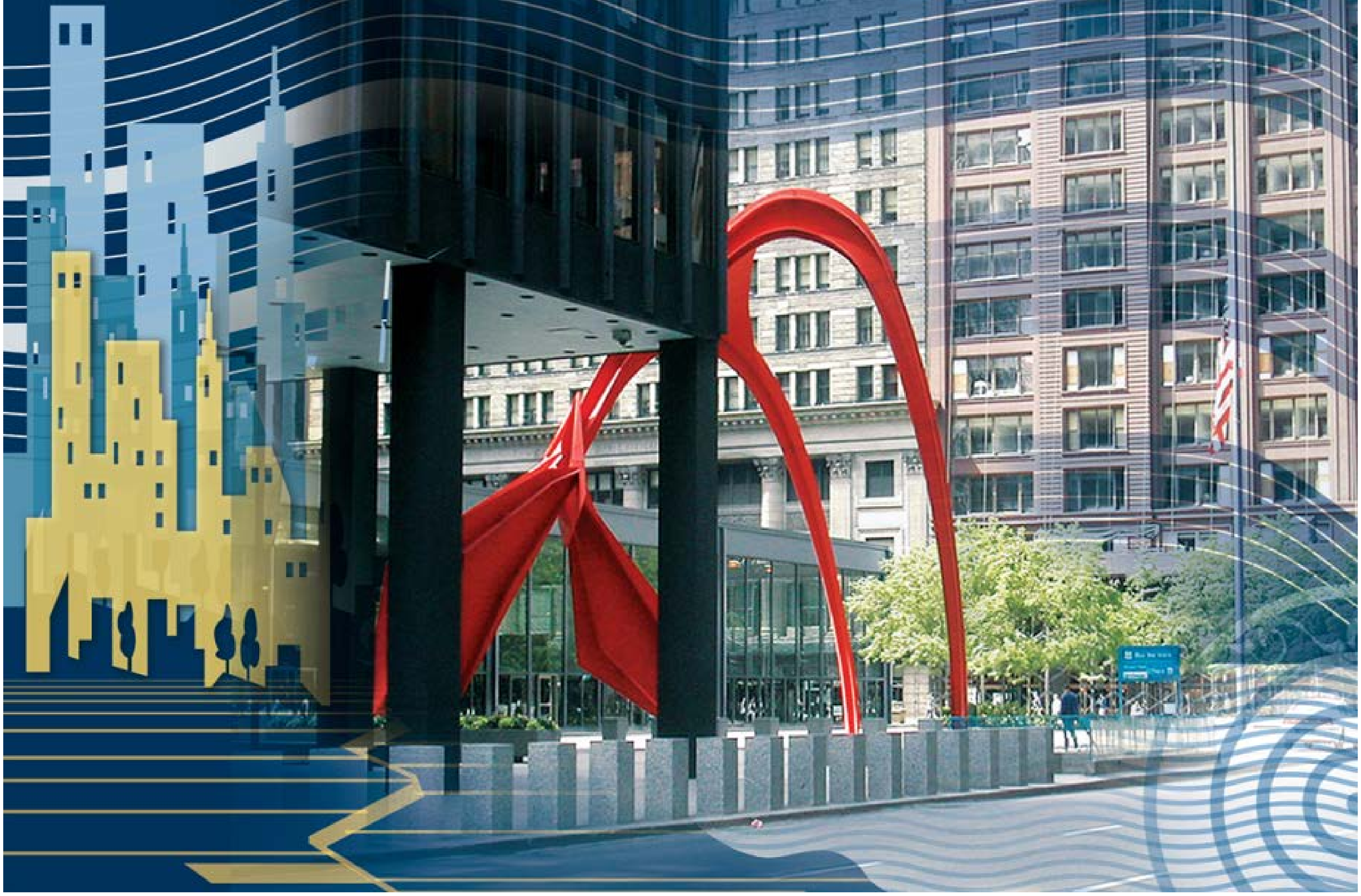


System Assessment and Validation for Emergency Responders (SAVER)

Access Control Technologies Handbook

September 2015

Homeland Security
Science and Technology

U.S. Department of Homeland Security
SAVER
System Assessment and Validation for Emergency Responders

Prepared by Space and Naval Warfare Systems Center Atlantic

The *Access Control Technologies Handbook* was funded under Interagency Agreement No. HSHQPM-14-00064 from the U.S. Department of Homeland Security, Science and Technology Directorate.

The cover photo is courtesy of FEMA. All other images included herein were provided by Space and Naval Warfare Systems Center Atlantic, unless otherwise noted.

FOREWORD

The U.S. Department of Homeland Security (DHS) established the System Assessment and Validation for Emergency Responders (SAVER) Program to assist emergency responders making procurement decisions. Located within the Science and Technology Directorate (S&T) of DHS, the SAVER Program conducts objective assessments and validations on commercially available equipment and systems, and develops knowledge products that provide relevant equipment information to the emergency responder community. The SAVER Program mission includes:

- Conducting impartial, practitioner-relevant, operationally oriented assessments and validations of emergency response equipment
- Providing information, in the form of knowledge products, that enables decision-makers and responders to better select, procure, use, and maintain emergency response equipment.

SAVER Program knowledge products provide information on equipment that falls under the categories listed in the DHS Authorized Equipment List (AEL), focusing primarily on two main questions for the responder community: "What equipment is available?" and "How does it perform?" These knowledge products are shared nationally with the responder community, providing a life- and cost-saving asset to DHS, as well as to Federal, state, and local responders.

The SAVER Program is supported by a network of Technical Agents who perform assessment and validation activities. As a SAVER Program Technical Agent, the Space and Naval Warfare Systems Center (SPAWARSYSCEN) Atlantic has been tasked to provide expertise and analysis on key subject areas, including communications, sensors, security, weapon detection, and surveillance, among others. In support of this tasking, SPAWARSYSCEN Atlantic developed this *Access Control Technology Handbook* for use by the emergency responder community. Access Control Technologies fall under AEL reference number 14SW-01-PACS titled System, Physical Access Control.

For more information on the SAVER Program or to view additional reports on access control or other technologies, visit www.firstresponder.gov/SAVER.

POINTS OF CONTACT

SAVER Program
U.S. Department of Homeland Security
Science and Technology Directorate
FRG Stop 0203
245 Murray Lane
Washington, DC 20528-0215

E-mail: saver@hq.dhs.gov
Website: www.firstresponder.gov/SAVER

Space and Naval Warfare Systems Center Atlantic
Advanced Technology and Assessments Branch
P.O. Box 1900222
North Charleston, SC 29419-9022

E-mail: ssc_lant_saver_program.fcm@navy.mil

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

PREFACE

This *Access Control Technologies Handbook* provides emergency responders, military and law enforcement security managers, and other security professionals with a reference on personnel and vehicle access control technologies, capabilities, and limitations. This handbook provides introductory-level information on the technologies and components for physical access control, as well as an overview of operating principles and applications. This handbook does not cover logical access control.

Most of the access control systems currently used in the security field are commercial off-the-shelf (COTS) products and have been successfully integrated into a wide range of other security systems. Efforts to acquire or use access control technology should be undertaken only in consultation with organizations or individuals experienced in this technology.

The data presented in this handbook has been restricted to those elements of an access control system that relate to personnel and vehicle access. Definitions of terminology commonly used and/or associated with access control technologies are provided in Appendix A.

The U.S. government did not conduct independent tests of any access control technology products or systems in developing this handbook and does not warrant, guarantee, or endorse any specific products. This handbook should not be considered definitive for use in planning or implementing an access control system. Such efforts should be undertaken only in consultation with organizations experienced in the various phases of planning, installing, testing, operating, and maintaining access control systems.

1. INTRODUCTION

This *Access Control Technologies Handbook* is a reference to be used during the planning and design of access control systems. This technology handbook is intended for use by emergency response personnel, disaster control personnel, civil disaster administrators, and local, state, and federal security and law enforcement agencies.

This handbook provides basic information to organizations whose primary functions may not encompass designing, evaluating, or installing access control systems, but need introductory level information related to the purpose, operation, and application of these types of systems. Any organization seeking to implement an access control system should do so only with the assistance of personnel or organizations that specialize in designing and installing such systems. Establishing an access control system involves not only design, installation, integration, and testing, but also the long-term issues of operation, training, and maintenance.

1.1 Organization

The handbook is organized into four sections. Section 1 is the introduction that describes the document's goals and objectives. Section 2 is an overview of the factors to be considered prior to selecting a suite of access control equipment. Section 3 provides an overview of the major equipment categories and reviews each of the personnel and vehicle access control technologies. This section describes the technologies, how they operate, how they are applied, their performance metrics, and their possible vulnerabilities. Section 4 provides guidance on selecting qualified vendors to assist the user in designing and/or implementing an access control system.

This handbook is best used by referring to the category overviews in Section 3 to determine which set of technologies might be most appropriate for the user's needs, and then reviewing the material on the individual technologies in the appropriate categories.

1.2 Objectives of Access Control

There are four objectives in access control that are part of an integrated physical protection program:

- Permit authorized persons to enter and exit; and deny entry to unauthorized persons. The systems covered in this handbook deal primarily with this aspect of access control.
- Prevent entry of contraband material, such as weapons, explosives, and tools, or the entry or exit of any other material restricted by security management. (Note: this handbook does not cover such equipment or methods.)
- Notify security personnel of attempts to gain unauthorized access or to tamper with or bypass the access control equipment. Some access control systems are capable of detecting these attacks, but surveillance and intrusion detection systems are also prudent supplemental technologies to consider.
- Maintain records of access control system activity, user permissions, and facility configuration changes.

2. ACCESS CONTROL SYSTEM CONSIDERATIONS

2.1 Categories of Equipment

The access control equipment discussed in this handbook is divided into four categories:

- Physical access control systems are the equipment used to selectively restrict access to a location. Physical control equipment usually begins the access control process at a distance outside a facility's perimeter mainly by controlling vehicular movement and pedestrian access near points of entry. For higher security applications, access control continues at building entrances and secure area entrances.
- Token and cipher systems are mechanical devices or electronic systems that facilitate authentication for the bearer to enter a protected space. A token is a physical device (i.e., ID card or key fob) that is kept on the user's person for use with the token system. Cipher locks perform a similar function using a personal identification number (PIN), or code, that must be keyed in for access.
- Biometric systems use physical or behavioral data measurements to determine authorization for access.
- Assistive technologies involve the use of alternative or specially designed equipment or implementation of special systems that enable personnel with disabilities to use the access control system.

2.2 Operational Requirements

Access control systems should be tailored to the needs and requirements of the resource or area to be protected. The starting point for defining needs and requirements is to perform a threat and vulnerability assessment. The type of facility, the nature of the environment, the organization's previous experience with access control systems, and assumptions about potential threats will influence the approach used to develop a solution. Other factors that should be considered in the vulnerability assessment are the nature of activity in and around the site; the size of the authorized population, varying degrees of accessibility, the physical configuration of the facility, the surrounding natural and human environment, fluctuations and variations in the weather, and training and support. An experienced access control system professional is an essential member of any program planning or vulnerability assessment team.

There are four main elements of an access control system:

- A barrier (e.g., vehicle gate, turnstile, door)
- Verification equipment (e.g., card reader, biometric scanner)
- A panel that controls the barrier
- The communications infrastructure that connects these elements and connects the system to the reaction elements, such as an alarm monitoring system.

Many access control systems incorporate surveillance equipment to allow security personnel to assess an entry alarm and to dispatch response personnel to evaluate the alarm, manage the access problem, or deal with any threat. A common choice for an assessment system is a closed- circuit television (CCTV) camera system. In some applications, access control systems

for personnel and vehicles are used in conjunction with a set of physical barriers and intrusion detection sensors. In order to operate, monitor, and maintain an access control system effectively, trained personnel are required. An equally professional team is needed to assess and respond to system alarms. Some questions that may be considered before acquiring an access control system are shown in Table 2-1.

Table 2-1. Questions to Consider When Acquiring Access Control Devices

1.	Will the system provide physical access control?
2.	Will the system integrate with an existing access control system?
3.	How many access points require coverage by the access control system?
4.	What are the threats to the facility (i.e., terrorists, angry ex-coworkers, theft)?
5.	What are the highest value assets that need to be protected? a. High value material property? b. Intellectual property? c. Classified intelligence?
6.	Where are the sites of greatest vulnerability?
7.	What areas require additional restricted access?
8.	Do the controlled areas contain an adequate information technology (IT) infrastructure?
9.	Should the access control technology have multiple functions?
10.	Are cipher locks required?
11.	Is a centralized network system required to monitor and program electronic locks?
12.	To what state will the system default in an emergency? (i.e., fail safe [unlock] or fail secure [lock]?)
13.	Does the organization have a written policy for evacuation, and will the access control system be used for mustering?
14.	Is automatic or remote operation of locks required?
15.	Does the security budget cover regular maintenance, training, and upgrades to the system?
16.	Does the system's installer or vendor provide adequate training to operate the system?
17.	Does the system include software or network access that will require certification and/or accreditation by IT professionals?
18.	What impacts do updates or patches to the access control software/firmware have on sustainment, testing, and/or certification?
19.	What preventative maintenance is required and how often should that be performed?
20.	Does the system include new or emerging technologies?
21.	What is the system reliability?
22.	Is cost effective vendor maintenance available?

2.3 Performance

The performance measure that characterizes all the categories of access control equipment in this handbook is throughput—the measure of the number of authorized persons or vehicles that can process through an ingress or egress point within a period of time. Throughput is one of the system capabilities that must be weighed against a facility's security needs. Some of the most sophisticated equipment can allow quite high throughput rates. In general, the higher the security requirement and the greater the number of access control devices one must pass through, the lower the throughput rates. The performance of biometric systems is generally based upon the number of data reading errors or false identifications. Those errors are defined and discussed in the biometric section's overview in Section 3.3.3.

2.4 Architecture

The architecture of an access control system should be developed as an integral part of an overall security system. In general, access control infrastructure consists of the following elements:

- Intrusion detection
- Surveillance
- Communications
- Response systems.

Access control may start at some distance from a facility's perimeter using features of terrain, roadway geometry, barriers, direction indications, and other mechanisms to guide vehicular traffic. Figure 2-1 is a sample access control schematic. Direct interaction with access control systems normally begins at entry points around a facility's perimeter. At this point and at locations inside, access control may be manual or automated in some fashion. Manual controls still rely on the access control systems for verification prior to manual authorization, such that a guard could use a CCTV camera and intercom placed near the barrier to identify personnel. Automated equipment may have an entire database resident at the site of the equipment, or the access control device may communicate with a centrally located or remote database. The manner in which authorized user data is handled at any location depends on the overall system and equipment choices and should be carefully considered with access control professionals during the design process.

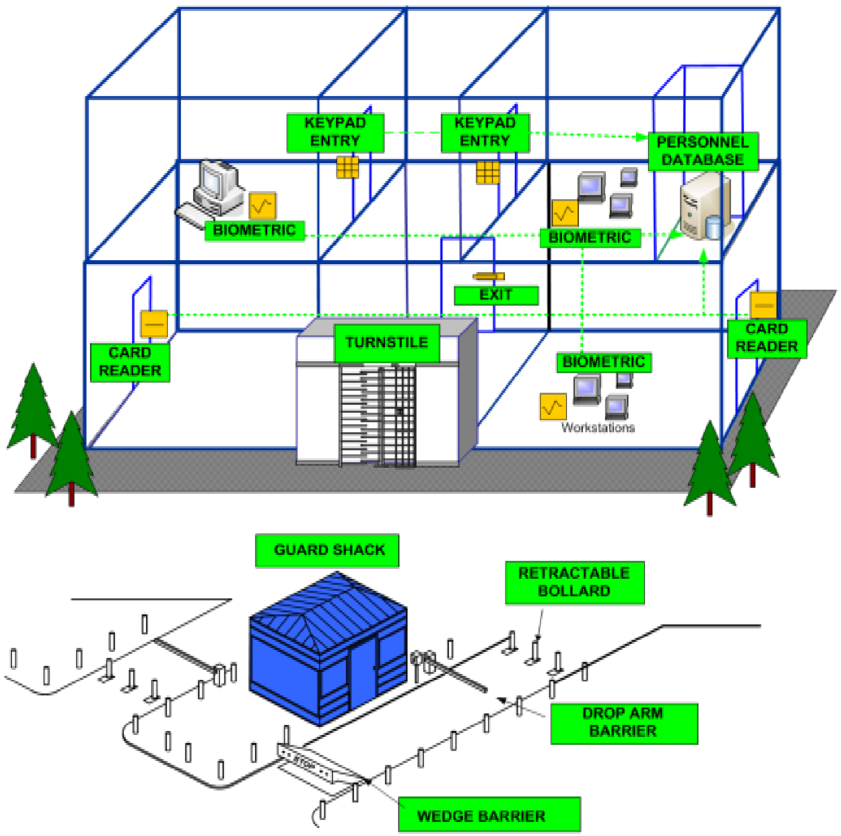


Figure 2-1. Access Control Schematic

2.5 Databases

Data regarding personnel authorized to enter parts of facilities may be paper-based, electronic, or both. Small facilities or those that have relatively low-security requirements may use personnel to manage the information by hand. Many facilities continue to meet their access control needs with security guards and identification badges or a token driven turnstile system that does not query a database. Most electronic token and biometric systems interact with automated databases. The operational portions of these databases often maintain just the information reference record used to verify or identify the user. Personal information used to generate the record may reside in archives or may be discarded after the records are generated.

Some electronic token and biometric access control systems can verify at the reader without querying the central database. Microprocessor smart cards may carry their own authentication algorithms and templates. Other systems' templates are small enough that the entire database can reside in the readers. The central databases may be less vulnerable to penetrations in such systems.

Centralized electronic databases are used primarily to manage the pool of authorized personnel and their access privileges and to maintain a record of ingress/egress events. Some software systems allow access privileges to be linked to security threat posture levels, organizational requirements, or other criteria, so that a change in criterion will automatically update the access privileges of each authorized individual.

2.6 Environmental

Many access control zones may have unique environmental characteristics that must be considered when designing the system, selecting the equipment, and performing the installation. Failure to consider all the factors can result in unacceptable performance, low reliability, or a short useful life. Exterior zones are likely to be affected by the prevailing climate, seasonal extremes, and fluctuations in weather conditions. Man-made environmental factors, such as activity patterns, electrical fields, radio transmissions, and movements of vehicles, trucks, trains, or aircraft also influence the design and performance of integrated security and access control systems. Interior zone access control equipment will generally be located in more controlled climates, but several environmental factors, such as electronic interference, must still be taken into account.

2.7 Alarm Monitoring Systems

In addition to the commercial off-the-shelf (COTS) access control technologies that are discussed in this handbook, there is a variety of alarm monitoring systems available. State-of-the-art systems provide visual and audible indications of an alarm. The alarm data is displayed on a computer monitor as text or as symbols on a map of the area. In most automated electronic access control systems, several of these capabilities are combined to provide the security operations center personnel with access control and intrusion detection information. Although each access control system is unique in the number and scope of options available, all automated systems perform the basic function of annunciating alarms and displaying the alarm locations in some format.

The control function of most of these systems is configured on a computer running any of the most popular operating systems, such as Linux®, Mac OS X®, UNIX®, or Windows®. Some operate with proprietary software, written by the manufacturer of the access control system. Most of the new security systems have links to mobile devices for accessing system information.

2.8 Alarm Assessment

Assessing an access control system alarm involves evaluating the alarm and analyzing audible and visual data to determine if an unauthorized access has been attempted or has occurred. The operator performs an assessment using CCTV, thermal imagery, and sometimes response force observation. Typically, the alarmed area is automatically displayed on monitors in the operations center and systematically recorded for future detailed analysis. The operator dispatches the response force if required. Some control systems can direct the CCTV or thermal imaging cameras toward a zone to provide the security personnel with a real-time view of the situation, to track the progress of an unauthorized access, and to hand off to adjacent monitoring and surveillance components as an intruder moves to other zones.

Incorporating mobile devices and laptop computers into many security command and control systems by using wireless technologies provides the responder with the same information as the central monitoring personnel. These capabilities significantly enhance the safety of responding personnel and allow for more efficient and appropriate responses to actual or suspected unauthorized access attempts.

2.9 Integration

Many current technologies have made integrating multiple access control devices into a cohesive security system more feasible. Integration of access control technologies with other systems or technologies may require the development of a software interface unless the system has been designed to operate with other technologies. Many companies offer equipment designed to work with a variety of access control, intrusion detection, and security systems and provide an interface control document (ICD). The equipment ICD identifies requirements associated with the access control system and its interface with other technologies.

All access control technologies have vulnerabilities and may generate false acceptances or rejections. Generally, access control systems should be supplemented with multiple access control technologies to protect against the weaknesses of any one technology, to enhance the system's overall effectiveness, and to provide means for security personnel to assess alarms and attempts to gain unauthorized access. Many access control systems have the capability to notify security personnel of attempts by unauthorized persons to gain entry; to tamper with, cut, or bypass the access control equipment; or to attack the connectivity between the access control equipment and the processing or command and control stations. Different access control devices can be integrated to reduce the chances of false acceptances and to provide alternatives for false rejections or inabilities to use a certain type of system.

2.10 Communications

Communications between the command and control unit and the access control devices may employ a variety of standard communications protocols. The building automation and control networks (BACnet) protocol is often used for access control systems. The protocol provides mechanisms for building automation devices to exchange information. It is an International Standards Organization (ISO) standard protocol, which includes Recommended Standard 232 (RS-232), RS-485, Ethernet, Attached Resource Computer Network (ARCNET), and point-to-point communications. Occasionally a manufacturer will use a proprietary communications protocol that may limit the possibility for future upgrades and system expansions to the original manufacturer.

2.11 Power Requirements

Regardless of the quality of design and installation, most access control systems are vulnerable to electric power losses. Some systems may not be able to reset automatically and could require operator intervention to restore operation, while other systems may require time to return to full operational status. Potential intruders may be aware of these vulnerabilities and may seek to cut or interrupt power if they cannot circumvent the system by other means. It is critical that all elements of the system have backup power systems incorporated into the design and operation to ensure uninterrupted operation, alarm reporting, situation assessment, and intrusion response. Backup power sources may include uninterruptible power supplies, generators, or automatic bus power transfer switches.

Power, line conditioning, and battery or other backup power requirements should be defined during the system design phase.

2.12 Costs

The overall costs of an access control system can be difficult to estimate and should be based on life cycle considerations. A vendor's bid may represent only the hardware cost, and may not include the costs of engineering design, construction, installation, testing, training, or maintenance.

Often the costs associated with infrastructure changes or the assessment and alarm reporting systems are more than the costs of the access control components. Costs can be minimized by defining threats carefully, performing a detailed site survey, and selecting between several technologies that provide similar categories of protection. Additionally, using suitable existing infrastructure, such as power cabling or conduit, can help mitigate some costs. Upgrade costs can sometimes be mitigated by choosing equipment compatible with existing systems or with parts of existing systems.

3. ACCESS CONTROL TECHNOLOGIES

3.1 Physical Access Control

Physical access control begins at the perimeter of a high-risk facility and is designed to restrict access and protect the employees and building functions and services from outside threats. The key element in protecting buildings is the establishment of an appropriate stand-off distance depending on the vulnerability assessment and the building characteristics. The first line of defense is the design of roadways, approaches, and parking areas in proximity of the building. The topics covered in this section are barriers, bollards, turnstiles and portals, and guard facilities.

3.1.1 Barriers

Barrier devices control vehicular access to specified areas while providing various levels of security to the facility. Barriers generally protect and control vehicular entry points by allowing only authorized vehicles. Many styles of barriers are available, such as wedge or drop arm barriers as well as ornate gates and planters. Retractable or removable barriers are available for situations where occasional access may be needed for authorized or emergency vehicles.

Barriers primarily prevent unauthorized vehicles from entering a controlled area by blocking the route of travel. They can also be used to guide or slow traffic near a controlled area, deter vehicles by their presence, absorb the impact of a vehicle, and/or damage a vehicle during intrusion attempts. There are several types of barriers available for specific applications, such as ornamental barriers at the edge of sidewalks and retractable barriers for emergency vehicle access to pedestrian areas.

A barrier's form, size, and design features vary with the level of protection necessary. Most traditional barriers are made of steel, concrete, or a combination of both and can be set above or below ground. Barriers can be active or passive. Active barriers are manually or automatically activated in response to acts of aggression. Passive barriers do not depend on detection or response and are usually stationary structures. Passive barriers are usually used for perimeter protection and at entry points that are rarely used or have restricted traffic.

3.1.1.1 Crash Gates

Crash gates are steel gates that slide across a roadway either on a track or through a roadside guide. They are used to stop unwanted vehicle traffic. When the vehicle is authorized, the gate opens to let the vehicle through. Crash gates are an effective defense mechanism and can be architecturally appealing.

3.1.1.2 Ground Retractable Automobile Barrier

The ground retractable automobile barrier (GRAB®) system, as shown in Figure 3-1, is an active vehicle barrier, which utilizes steel cables and energy absorbing pistons to stop vehicles while injury to vehicle occupants is minimized. It is designed to be reset and back in operation after an impact. Due to its energy absorbing capabilities, the system provides security while preserving much of the integrity of the barrier. This is an important consideration as many barriers are destroyed after a vehicle impact, leaving the site vulnerable while the barrier is restored.

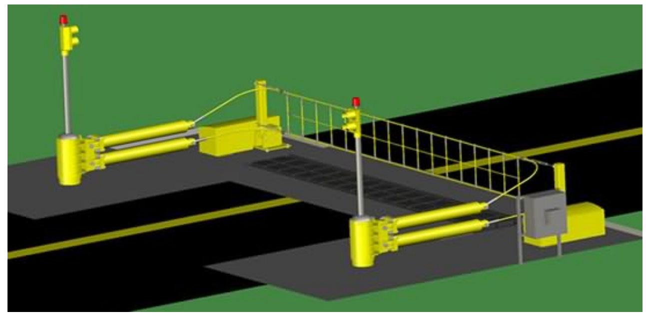


Figure 3-1. GRAB 300

Image courtesy of FutureNet Security Solutions, LLC

3.1.1.3 Wedge

Wedge barriers, as seen in Figure 3-2, are hydraulically operated steel devices that angle upward from ground level to create an impregnable edge above the surface of the road. A retracted wedge barrier forms part of the road surface. Once deployed, a wedge barrier makes a 45° angle from the road surface facing the direction of vehicle movement and is coupled to a foundation pad to absorb the kinetic energy from an impact. These devices are very effective against an attempted vehicular breach.

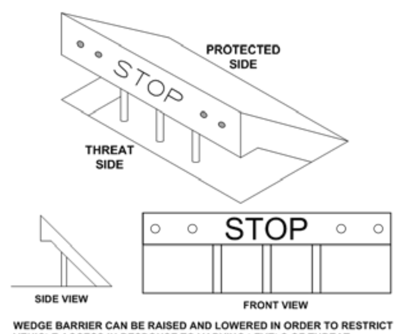


Figure 3-2. Wedge Arm Barriers

3.1.1.4 Drop Arm

Drop arm barriers, as seen in Figure 3-3, are commonly used at parking lots and garages to control entry and exit of authorized vehicles. The arms of some products are capable of stopping unauthorized vehicles when in the down position. Some drop arm barriers incorporate a cable designed to lasso and destroy the front end of a vehicle attempting a breach.

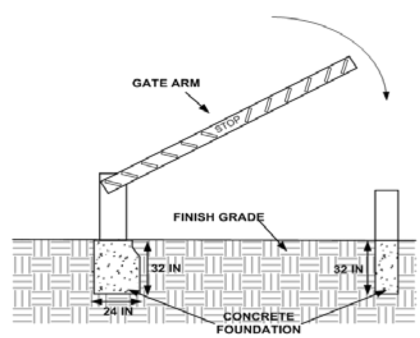


Figure 3-3. Drop Arm Barriers

3.1.1.5 Portable Wedge

Portable wedge barriers can be set up in as little as 15 minutes to a few hours without the need for excavation. The crash protection ratings of portable wedges are often lower than those of permanent barriers, but they are still very effective. Portable wedge barriers often sustain significant damage in a vehicle impact and may need to be repaired or replaced after an incident.

3.1.1.6 Applications

Barriers are used as a physical obstacle to block or restrict access to an area. Some applications of barriers are:

- Interior barriers are useful in warehouses, parking garages, and other interior environments where vehicles are present. Barriers may be placed to protect critical infrastructure, such as power control units or air conditioning units. They may also protect pedestrian access areas or slow the progress of vehicular traffic through an area.
- Exterior barriers are primarily used for exterior applications at any facility to help regulate vehicular traffic and to stop deliberate intrusion attempts.
- Portable barriers are useful for temporary perimeter and access control situations. They cover a range from lightweight plastic devices to concrete versions that must be moved using mechanical lifting equipment. Lightweight plastic versions are often brightly colored, can be water filled, and are used in the same manner as traffic cones to warn the public of hazardous conditions or of temporary vehicle access restrictions.

3.1.1.7 Performance Metrics

U.S. federal agencies have developed systematic test standards using real crash tests to quantify, verify, and certify barrier performance. These test methods were initially published and maintained by the U.S. Department of State (DoS) in 2003 as SD-STD-02.01 Revision A, which has been replaced since 2009 with *ASTM F 2656-07 Standard Test Method for Vehicle Crash Testing of Perimeter Barriers*. To obtain certification, manufacturers must have their products tested by independent crash test facilities to demonstrate that they meet ASTM standards. This test method provides a structured procedure to establish a penetration rating for perimeter barriers subjected to a vehicle impact. Knowing the penetration rating can help agencies select an appropriate barrier for site-specific conditions around a facility.

3.1.1.8 Vulnerabilities

Barriers are often used to establish a stand-off distance for vehicle access to an area. This is a common adversary delay time tactic; however, barriers should be complimented by an electronic sensor system that relays detection information back to a monitoring system.

3.1.2 Bollards

Bollards limit vehicular access to specified areas while providing various levels of security to facilities and pedestrians. Bollards allow unimpeded pedestrian passage, unlike barriers. Bollards come in a number of styles and provide different levels of security with a variety of aesthetic characteristics. Retractable or removable bollards are available for situations requiring

only occasional access for authorized or emergency vehicles. Bollards can be constructed of concrete, steel, cast iron, or plastic in a variety of forms and sizes. Bollards have become more prevalent in facility designs because of their high level of public acceptance. They guide and deter vehicles by their presence, but do not impede pedestrian traffic. During vehicular intrusion attempts, bollards absorb kinetic energy and inflict vehicle damage.

3.1.2.1 Fixed Bollards

Fixed bollards, as shown in Figure 3-4, offer a high degree of cost effective protection. They are commonly placed in and around airports, federal buildings, and other public facilities where vehicle control is required, but foot traffic must be unimpeded. Fixed bollards are generally made from tubular steel or cast iron. Some are filled with concrete for added strength. The subsurface engineering of fixed bollards depends on the required level of protection.

3.1.2.2 Removable Bollards

Removable bollards may be required to create an emergency access route through a controlled perimeter or to increase security on an occasional basis. Removable bollards lock into place and often have a cap to cover the foundation when the bollard is removed. These devices are generally less protective than fixed bollards, because the foundation is less robust.

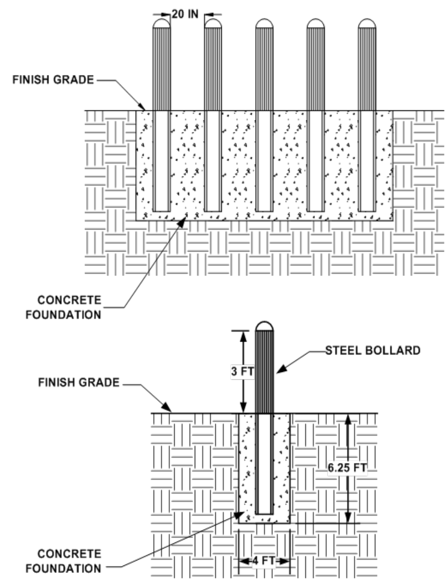


Figure 3-4. Fixed Bollards

3.1.2.3 Retractable or Automatic Bollards

Retractable bollards, as shown in Figure 3-5, are generally operated by hydraulic or pneumatic power units and can be lowered into the ground to allow authorized or emergency vehicles to pass. These bollards can return to full height in the event of a security threat. A manual method of operating them during a power or system failure is a standard feature. The subsurface engineering depends on the required level of protection.

3.1.2.4 Manual and Semi-Automatic Removable Bollards

Manual and semi-automatic bollards cost less than fully automatic bollards and offer similar access control effectiveness. These devices may be suitable when the quick response of automatic bollards is not necessary. Semi-automatic bollards must be unlocked to change the position from raised to retracted or vice versa.

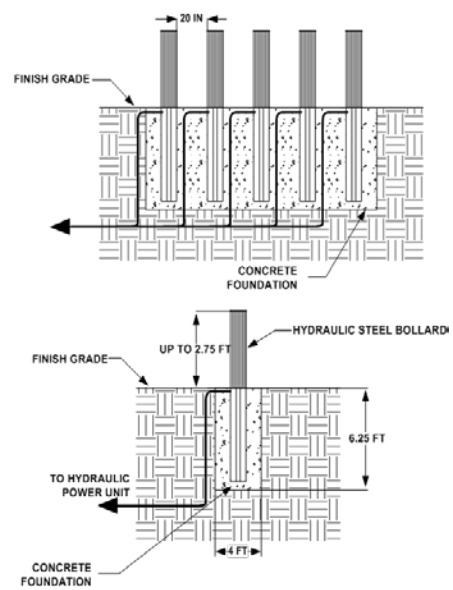


Figure 3-5. Retractable Bollards

Compressed gas is often used to raise a semi-automatic bollard; although a hand crank or pull system may also be used. Manual and semi-automatic bollards are essentially designed and installed in the same manner as automatic bollards, differing only in the manner in which they are deployed.

3.1.2.5 Portable Bollards

Portable bollards range from lightweight plastic devices to concrete versions that must be moved using lifting equipment. Portable bollards generally do not attach to a foundation. Lightweight plastic versions are often covered with reflective tape and are used in the same manner as traffic cones to warn the public of hazardous conditions or of a temporary denial of vehicle access. They may be used to restrict vehicular traffic temporarily for a parade or other social event.

Portable concrete bollards require mechanical assistance for transportation and placement. These are often used to augment vehicular access control during periods of increased security threat levels.

3.1.2.6 Applications

Bollards are primarily used for exterior applications, but are useful in interior applications where vehicles may be present, such as warehouses, parking garages, arenas, or stadiums. In building interiors, bollards may be placed to protect critical infrastructure such as power control units, air conditioning units, pedestrian access areas, or locations where a separation between vehicle and pedestrian traffic is needed.

In exterior applications, bollards can be used to define a vehicle free area or to restrict vehicle traffic from certain routes and roadways. Typical uses of portable bollards are to protect parking spaces, prevent vehicles from blocking a driveway, or provide a warning of a safety hazard.

3.1.2.7 Performance Metrics

ASTM International Designation F 2656-07 defines systematic test standards using real crash tests to quantify, verify, and certify barrier performance. Prior to receiving certification, manufacturers must have their products tested by an approved independent crash test organization to demonstrate that they meet ASTM standards.

3.1.2.8 Vulnerabilities

When it comes to bollards, visibility is the most important safety issue. Retractable bollards may be triggered without a pedestrian noticing. Many vendors offer custom colors which make the bollards more visible. Most bollards have highly reflective labels which help further improve visibility.

3.1.3 Turnstiles and Portals

Turnstiles and portals manage pedestrian traffic flow and access at checkpoints. Turnstile technologies range from a simple, stand-alone rotating tripod with no accounting functions to electrically activated barriers with optical scanners that are components of fully automated access control systems.

Portals are electrically controlled gates or doors used as controlled openings in a physical barrier. Portals can be used singly or in sets to form mantraps as a delay device. Mantraps, as shown in Figure 3-6, are an arrangement of doors, usually forming a small corridor or booth, which allows a person to enter and be identified before proceeding into a controlled area. They are often used in high-security applications that require individual scrutiny and can tolerate low throughput rates.

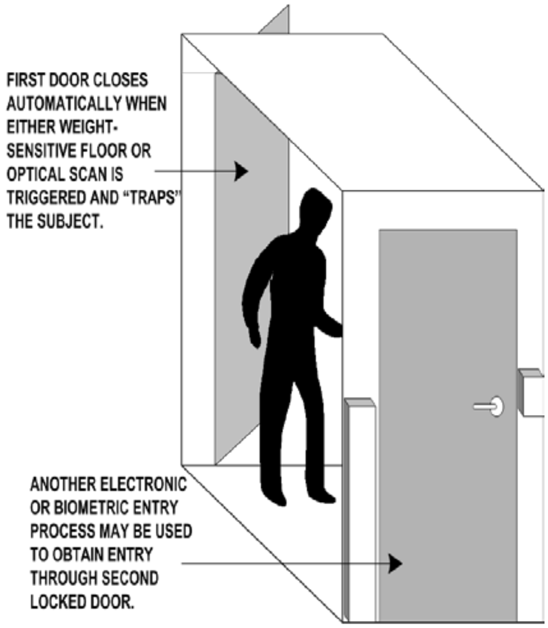


Figure 3-6. Mantrap

Turnstiles and portals encourage employees and visitors to abide by access control procedures and reduce the need for security personnel to monitor ingress and egress points. Some products provide information on the direction of travel and can count the number of pedestrians. Often the access approaches are arranged using markings or railings so that people awaiting access will form a line. Most manufacturers include audio or visual prompting devices to indicate the direction of travel and alarms for attempts to enter without authorization.

3.1.3.1 Operation

Turnstiles operate in many different ways. In each application, they limit access using various barriers that revolve, rotate, retract, or lever, as shown in Figure 3-7. Many include provisions for additional access control devices including smartcard, proximity, and biometric devices. While full-height turnstiles may be used in high-security settings, waist high turnstiles are the most common.

In both turnstile and portal operations, a pedestrian approaches and walks through or, may swipe a card, wave an access card by a reader, or enter an access PIN on a keypad before walking through. The access control system compares the data entered with the enrollment database and, if entry is authorized, signals the portal to open or the turnstile to release and allow access.

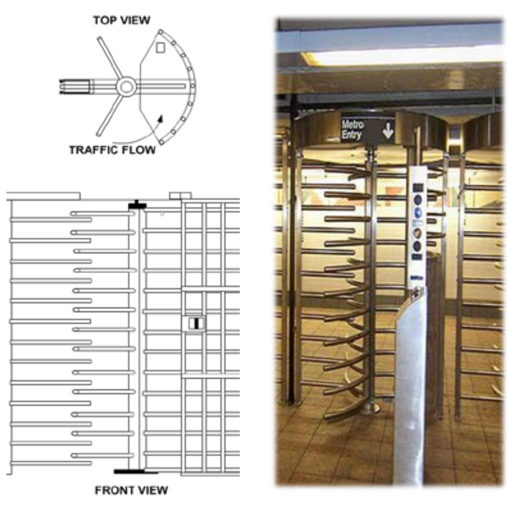


Figure 3-7. Turnstile

Some portals have optical scanners or weight-sensitive floors that register a pedestrian's entry to the access entry lane and regulate tailgating, which is when a second person follows closely behind without detection by the access control system. These access control systems usually have an anti-passback feature that prevents an individual from passing their card or badge back to an unauthorized person attempting to gain access. The system shows the individual as in or out. Once in, the system will not allow the same card to enter again, and once out, the system will not allow the same card to exit again.

3.1.3.2 Applications

Turnstiles are used for pedestrian control in airports, schools, stadiums, arenas, perimeter and interior security, retail crowd control, transit fare collection, and lobby or building access control where high throughput is necessary. Portals are used in higher security situations in which more scrutiny of each individual is required. Portals are often interlocked as a mantrap when prolonged scrutiny is required of each person seeking access.

3.1.3.3 Performance Metrics

There is no single performance standard for turnstiles and portals. Most are equipped with safety features that allow mass egress in emergencies. Several manufacturers have equipment complying with the Americans with Disabilities Act (ADA) of 1990. The specific application of access control technology also influences the performance of equipment. Turnstiles have relatively high throughput, even though people must pass through the opening in a one-by-one sequence rather than as a crowd. Portals have lower throughput than turnstiles, because the device must open and shut for each person passing through.

3.1.3.4 Vulnerabilities

Turnstiles and portals may be vulnerable to tailgating. This can be avoided by incorporating additional security features.

3.1.4 Guard Facilities

Guard booths provide shelter for a facility's guard or access control personnel, as shown in Figure 3-8. A guard booth is often the first thing a visitor encounters upon entering a secure facility. Many booths on the market today combine aesthetic appeal with a high degree of strength and durability. A guard booth may be nothing more than a physical shelter against the elements, or may be a component of a secure fortress against physical attacks. High-security booths are available that meet or exceed commercial and federal standards for ballistic and explosion protection.

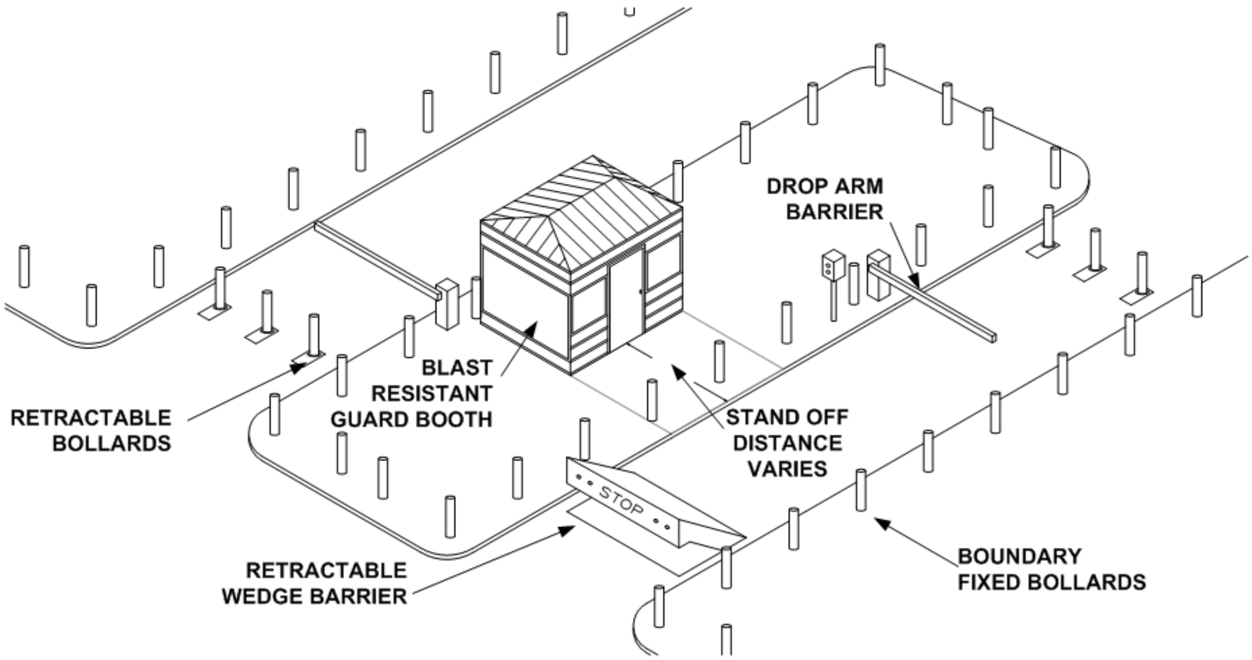


Figure 3-8. Guard Facility at Entry Point

3.1.4.1 Operation

A guard booth provides shelter and protects a facility's security forces from the weather and, based on security requirements, protects against some forms of attack. For high-security facilities, such as nuclear power plants or government facilities, guard booths may be the first line of defense against unwanted visitors or attacks. When combined with other physical access control devices, as seen in Figure 3-8, a facility can maintain a high degree of protection against a forced entry. High-security booths built to federal explosion resistance standards are designed to provide protection for the booth occupants during an explosion.

3.1.4.2 Applications

Most guard booths are located outside a facility at vehicle entry and personnel access points. Personnel greeting or visitor check-in points are prime interior locations for guard booths. They are often prefabricated according to the customer's security and aesthetic needs and shipped directly to a facility. Many options are available that range from sliding transaction drawers to full restroom facilities. Portable booths with various levels of ballistic and explosion protection are available.

3.1.4.3 Performance Metrics

Guard booths can be built to provide specific levels of protection against particular types of threats, most often firearms and explosions. Standards for ballistic or explosion protection have been developed by several U.S. government and commercial entities, such as the National Institute of Justice (NIJ) and Underwriters Laboratories (UL) for ballistic protection and by the General Services Administration (GSA) for explosion protection. Security managers requiring high-security guard booths should consider incorporating minimum standoff distances for explosives, vehicle barriers, and delay devices into the overall security infrastructure.

3.1.4.4 Vulnerabilities

Guard booths can be circumvented in order to gain access to a location and should be used with other means of security, such as perimeter fences and CCTV.

3.2 Tokens and Cipher Systems

There are at least three functional blocks in any mechanical or electronic token-based access control system: the token itself, the token reader, and an access control panel. The access control panel provides control signals to the security devices, such as electric or magnetic locks, based on input from the token reader.

A token is a physical device (i.e., ID card or key fob) that facilitates authentication for the bearer to enter a protected space. A token may be examined by security personnel or authenticated electronically by the token reader using a challenge/response cycle such as an electronic password or PIN, verifying a biometric sample, or using another algorithmic procedure.

A properly designed and installed token-based access control system can be used to monitor physical access, logical access (e.g., computer and network), employee time and attendance, as well as a number of other functions tailored to meet an organization's security and administrative requirements. Token-based access control has been widely used for many years.

The token systems discussed in this handbook vary in complexity, from simple to complicated, and for low to high security applications. Identification cards and badges are physical systems that require visual verification at an entry point to be effective.

Cipher systems allow personnel through a door after entering a multi-digit code. Key card systems only allow those who have a specifically coded key card to pass through a particular door.

The access control security level of a facility can be increased in three ways. One is to use more capable access control systems at each entry point. Another is to require more than one access control technology at an entry point. A common security process, known as two-factor authentication, is to present a token and require an additional piece of information that is usually memorized. For instance, to use an automated teller machine (ATM), one must present a bankcard to the machine and then enter a PIN using a keypad. A third way to increase access control security levels is to design layered systems, where fewer people have access to more sensitive areas inside the facility.

3.2.1 Identification Cards and Badges

Cards and badges are the most common form of identification used in the access control industry. Identification cards and badges are usually slightly larger than a credit card. They often have a picture of the holder, the holder's name, the organization's name or logo, and other pertinent information. Barcoding, holographic imaging, water marking, and time expiring chemistry are the primary technologies available to customize a particular identification badging system beyond the basic information and photo. Many card or badge systems can accommodate more than one of these customizing technologies.

3.2.1.1 Barcoding

Cards and badges with barcodes can accomplish keyless automatic identification and data collection for access control systems and are typically used in low security applications. Barcodes use vertical lines of varying height and width which represent an identification security code. The barcode is analyzed by the reader, verified against an access control list, and the card holder is allowed or denied access to the area. Several industries, specifically automotive, electronics, and chemical, have defined standards for their uses and applications. These standards ensure universal compliance within an industry and identification accuracy better than 99 percent.

3.2.1.2 Holographic Imaging

A hologram is an image printed on a card or on the card's lamination that uses light diffraction techniques to produce an image that can be seen, but not copied. The holographic image is used as an anti-forgery technology on badges; however, the equipment used to create these images can be expensive and may not be cost-effective.

3.2.1.3 Time Expiring Chemistry

Time expiring cards or badges use techniques to imbed reactive chemicals into the surface or the lamination. The chemicals react in a known time period and change color. Time expiring chemistry is useful for persons who should have only temporary access to a facility or area. A time expiring badge can be printed with information or images, including photos, and then the technology applied and activated. Time limits range from one hour to one month. When the time runs out, the color changes or bleeds through on all or some portion of the card or badge.

3.2.1.4 Watermarking

A watermark is an image in the surface or lamination that can be seen, but not copied, and can be used as an anti-forgery technology.

3.2.1.5 Applications

Identification cards and badges are first tier security tools. For many facilities, they are all that is required. Where guards are present to monitor access, persons entering frequently must show a facility badge or identification card. Visitors and other persons lacking badges are moved aside to apply for authorization to enter. Badge holders are often required to display their badge prominently throughout their time in the controlled area.

Cards or badges can be the basis for high-security access control systems that depend on using personnel and administrative techniques instead of electronic infrastructure. For example, some facilities use two photo identification badges for access control. The first badge is given to the portal control person, who matches it against a file of interior access badges. When a match is found, the guard exchanges the badges and allows the individual to access the facility. The second badge is to be visible at all times in the protected area. The badges are again swapped when the individual leaves the protected area. While this type of system does not rely heavily on technology, it does offer some advantages. The interior access badges never leave the protected area. When an access privilege is changed or revoked, the interior card is simply updated to reflect the new level of access.

3.2.1.6 Performance Metrics

Cards and badges are most often made from polyvinyl chloride (PVC) stock or rigid paper stock. PVC is durable, robust, and able to withstand a moderate amount of abuse. Heavy or rigid paper stock is usually laminated after printing. The process of issuing, showing, or wearing a badge provides a basic level of access control for many organizations. It identifies the persons authorized access to a controlled facility or services, and provides a quick, reliable means of visual identification.

3.2.1.7 Vulnerabilities

Cards and badges can fray, delaminate, or break while being carried, handled, or passed through readers. Since potential intruders may try to copy or substitute cards or badges, some facilities use holograms or watermarks to complicate the counterfeiting process. Cards and badges are also susceptible to loss and theft. Two-factor authorization, such as the card along with a password, a PIN, or biometric data, can help prevent an unauthorized person from gaining access with a lost or stolen card or badge.

3.2.2 Keycard Door Systems

Keycard door systems have a reader attached directly to a door and are an integral component of the latch control mechanism (Figure 3-9). They are often used in the hospitality and hospital industries to provide a relatively low level of security to client personnel in situations where each client needs authorization to open a few doors, perhaps his or her own room, and the building after hours. Door mounted key card systems do not interact in real time with a central database. Information on a door's activity is stored in a battery powered recording system inside the door-mounted box and must be downloaded into a hand held reader, which may then be downloaded into a central record keeping computer.

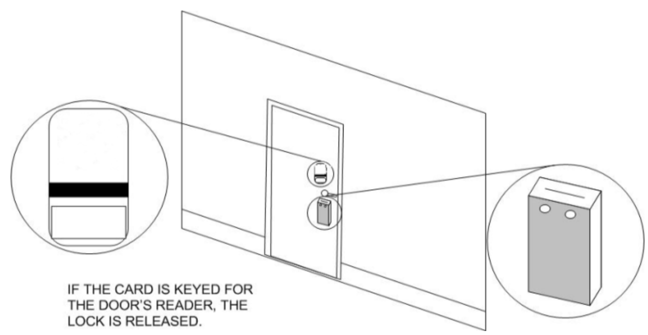


Figure 3-9. Keycard Operation

3.2.2.1 Operation

A user must insert a valid card (Figure 3-10) into the reader on the door to release the lock and allow entry. Each lock's reader and latch control mechanism is self-contained and is not connected to a remote access control panel or a central control system.

These systems are available in two technologies: magnetic encoded stripe and contact smart card. Systems using magnetic encoded stripes and contact smart cards require a key to be encoded at the point where the card is issued. The stripe normally contains about 140 digits and characters in one to three tracks, the user name, authorized access levels, expiration date, and other information.

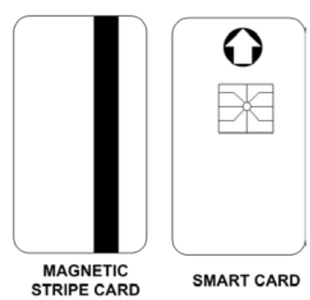


Figure 3-10. Types of Keycards

The quantity of information on contact smart cards can be much greater than on a magnetic encoded stripe card. The magnetic encoded stripe and contact smart card key card systems should not be confused with the systems capable of very high security access control covered in the technology reviews on magnetic encoded stripe systems and contact smart card systems.

Inserting a keycard into a lockset operates keycard locks. Some systems read the presence of a valid card in the slot, and will remain unlocked as long as the card is present. In other systems, such as magnetic encoded stripe, the card must be fully inserted and then removed to cycle the lock. Many systems have red and green LEDs on the lock face to indicate the state of the lock. When a valid card is detected, the green LED illuminates, the electric lock opens, and the user can operate the mechanical latch. Operating the mechanical latch completes the cycle and resets the lock to the closed position. When an invalid card is detected, the red LED illuminates, the electric lock will not open, and the mechanical latch remains locked.

3.2.2.2 Applications

Keycard systems are not often used in high-security situations because the readers typically do not interact with a central access control database; however, this technology allows flexibility and fine-grained access control. Fine-grained access control is the ability to permit or deny access through a single door or set of doors. For example, doors can easily be re-keyed whenever a key is lost or stolen, and access can easily be modified for special requirements. Room keys, staff keys, and manager keys can be coded to enhance both security and productivity. Room keys might operate a lock to the room and some common area, while a staff key could operate the locks for a series of rooms, but only within a certain time period.

Centralized control offers advantages in emergencies. Access for fire and emergency crews can be coordinated and granted to affected areas quickly. In systems where locks are under local control, having emergency policies set in advance can be beneficial. Master keys should be protected from misuse, but still be readily accessible when necessary to protect the lives and possessions of occupants. Fine-grained access control systems can also be used in schools, colleges, hospitals, public and private office buildings, and residences. Keycard technology is suitable for both interior and exterior applications.

3.2.2.3 Performance Metrics

The performance of keycard-based door locking systems is measured by the number of cycles before corrective maintenance is required. Vendors and manufacturers often advertise performance values near one million cycles.

3.2.2.4 Vulnerabilities

Properly engineered and maintained keycard systems are highly effective, especially when augmented with automated alarms and security monitoring and response forces. The magnetic encoded stripe on some keycards is vulnerable to strong magnetic fields, which can corrupt the encoded information. There have been additional concerns about the privacy of information on magnetic encoded stripe and contact smart card-type keycards; however, most systems only encode the access code and possibly the individual’s name on the card.

3.2.3 Cipher Lock

Gaining access using a cipher lock (Figure 3-11) requires memorization of a code or series of numbers. Door lock systems of this type may be mechanical, electronic, or electro-mechanical. Mechanical cipher locks normally attach to the door itself, while electronic cipher locks may be mounted on the door or on a wall next to the door they control. Electronic cipher locks control an electric strike, striker plate, or latch, and are operated by pressing a combination of buttons or rocker switches. The buttons are often located behind a shield to prevent the combination from being observed. The buttons on a mechanical cipher lock are arrayed in a circle or a vertical line near the knob that moves the bolt once the lock has been released. This knob is known as a thumb turn or deadbolt lever. Electro-mechanical cipher locks share the features of electronic and mechanical locks and may have a dial type combination lock.



Figure 3-11. Cipher Lock System

3.2.3.1 Operation

A user must press a valid combination of buttons or switches to release the lock and allow entry. A cipher lock is usually a self-contained unit, and operates without connection to a central control system or intermediate panel. Security personnel can change the combinations on mechanical and electronic locks. Some require special tools to change a combination, but such tools normally accompany the lock in a retail package.

Electronic cipher locks may have some features and capabilities that are not available on mechanical locks. Door mounted versions are usually powered by batteries and are self-contained. Some electronic locks allow multiple combinations and keep a record of events in an electronic memory consisting of the date and time that the lock was operated and the combination used. The multiple combination capability is an advantage because it allows each user to possess a unique access code. Newer electronic cipher locks provide additional functions through software and programming, such as the ability to download an event record into a mobile device.

Security managers can program electronic cipher locks to stay open during certain periods and not respond to entry requests during other periods such as holidays or after working hours. Wall mounted cipher systems use standard electrical power and offer many of the same capabilities as the self-contained door mounted versions. Some cipher locks feature the ability to randomize the label assignments to the keys in wall mounted units. Each time the lock is operated, the keys are labeled differently to prevent an observer from learning a combination by watching hand movements. Operating the door completes the lock cycle and resets the lock.

3.2.3.2 Applications

Cipher locks are predominantly found in access control applications requiring low to medium levels of security. They can be useful in high security situations when they are used in conjunction with access control systems that verify each user. Record archives, organizational file facilities, mailrooms, and spaces containing potentially hazardous materials, such as pharmacies or paint storage rooms, are examples of appropriate applications for cipher lock systems. These systems are also suitable for use in schools, colleges, public and private office buildings, and residences. Cipher lock systems can be used in both interior and exterior applications.

3.2.3.3 Performance Metrics

The performance of cipher lock systems is measured by the duration of time that the lock continues to perform under various adverse conditions, such as exposure to extreme heat, dust, or high humidity.

3.2.3.4 Vulnerabilities

Properly maintained and administered cipher lock systems are highly effective, especially when augmented with automated alarms, CCTV monitoring, and response forces. However, two important vulnerabilities must be noted. In cipher lock systems where many people use a single combination, the security manager can never be certain the combination has not been compromised. The combination for this type lock should be changed frequently to contain the effects of such a compromise. Using systems that support multiple combinations can also decrease this vulnerability. A second important vulnerability is locks requiring only three numbers in a combination can be defeated with persistence because there are only 1,000 possible combination results. Tailgating is another possible vulnerability unless users are trained to notice who is entering with them and to be certain that the door shuts after use.

3.2.4 Magnetic Stripe Cards

Magnetic stripe cards are tokens used for authentication and access control in many security environments. Magnetic stripe card readers can be interfaced with a variety of access control equipment, including locally controlled electrical locks, or centrally controlled security databases. Magnetic stripe cards are identical in composition and appearance to bank or credit cards. The stripe normally contains about 140 digits and characters, divided among one to three tracks in a proprietary format. They can double as identification cards or badges when they are printed or embossed with the user’s name, identification number, imprints of corporate or organizational logos, and a photograph.

3.2.4.1 Operation

Magnetic stripe cards must be either swiped through a reader track, as shown in Figure 3-12, or fully inserted and then removed from a reader in order to cycle a lock. Card readers can be mounted to adjacent walls, doorframes, or any convenient surface. Many systems include red and green LEDs on the lock face to indicate the state of the lock. When a valid card is detected, the green LED illuminates and the electric lock opens. When an invalid card is detected, the red LED illuminates and the electric lock will not open. Depending on the system, the control of the lock can be located at the door, at an intermediate control panel, or at a central control station to manage authentication processes for a large facility with many authorized users. Systems can be programmed so that an alarm is generated after a preset number of failed access attempts.

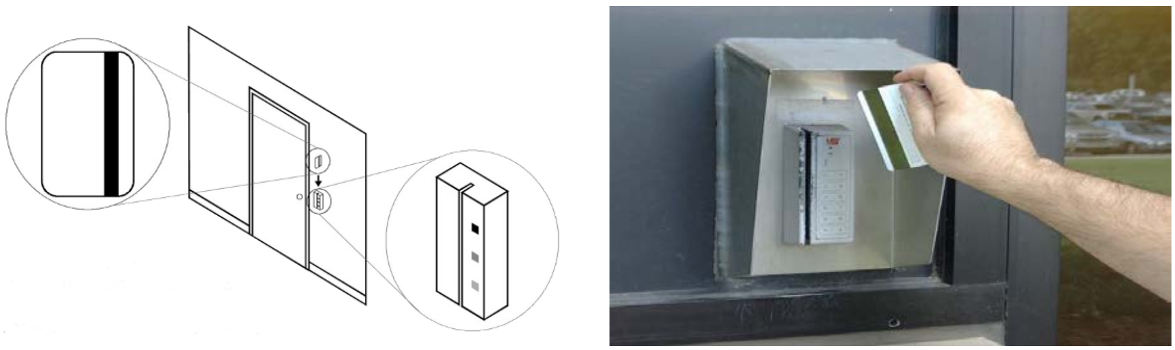


Figure 3-12. Magnetic Stripe Card

Magnetic stripe readers detect the points on the stripe where the magnetic encoding reverses polarity. Areas where two north magnetic poles or two south poles are adjacent cause a small voltage transient in the card reader. These transients, used in combination with clocking and error checking algorithms, produce a series of binary digits that can be used to represent binary coded decimals, a limited set of American National Standards Institute (ANSI) alphanumeric characters, or information in another proprietary or encrypted format. Caution should be used when selecting a magnetic stripe card reader, because many readers only read track one or track two, but not both. Encoding a magnetic stripe card is normally accomplished when a card is issued, using a card printer with the appropriate capabilities. Card printers are widely available.

3.2.4.2 Applications

Magnetic stripe systems are used throughout the public and private sectors, because of their relatively low cost and versatility. They are much more versatile than keycard systems. Essentially keycard systems provide local control of an access point, but lack the capability of centralized control. Often, keycard systems also lack recordkeeping capability; however, magnetic stripe systems offer both fine-grained control of access points and detailed, real-time record keeping capability.

Magnetic stripe systems achieve this using centralized system control. In centralized systems, the security manager maintains a computerized database of authorized permissions for each cardholder. When a cardholder operates a reader, the reader sends a signal back to the controller, which identifies the card-bearer and access point. If a card-bearer has permission for the door, then the access point opens. Another advantage of centralized control is that the list of

permissions for each user can change according to the situation. For example, the permissions of every user could be revoked if it became necessary to lock everyone out of a facility. Permissions for a single user could be revoked or modified during planned periods of absence such as vacation, holidays, business travel, or at certain times of the day. Automated, centralized access control also provides more accurate record keeping.

Centralized control offers advantages in emergencies. Access for fire and emergency crews can be coordinated and granted to affected areas quickly. Fine-grained access control systems can be used in schools, colleges, hospitals, public and private office buildings, and residences.

3.2.4.3 Performance Metrics

Like other electrical lock systems, the performance of magnetic stripe systems can be measured by the number of cycles performed before corrective maintenance is required or a card must be re-issued. Vendors and manufacturers often advertise high performance values; however, site-specific conditions (e.g., extreme heat, dust, high humidity) can cause the actual performance to be much lower.

3.2.4.4 Vulnerabilities

Equipment used to copy and encode magnetic stripe cards is commercially available; therefore, magnetic stripe cards can be copied and forged with relative ease. Additional features imprinted on the card such as identification photographs, corporate logos, and holograms all help to minimize the chance of an effective forgery. The information encoded on the magnetic stripe should differ from the information on the face of the card to prevent forgers from simply encoding the information from the card face.

There have been concerns about the privacy of information on magnetic stripe cards; however, many systems now encrypt personal information, leaving only the access code and possibly the individual’s name encoded on the card. Relatively weak magnetic fields can corrupt the encoded information on some cards, particularly the cards used with low-energy encoding devices. Cards that use high energy encoding have a magnetic medium with greater permanence and resistance to ambient magnetic fields.

3.2.5 Contact Smart Card

Access control systems using the contact smart card can be employed in high-security applications which involve large numbers of people that require significant flexibility and layering, but need only moderate throughput rates. These systems are replacing many of the key card and magnetic stripe systems due to their ease of use, security, and reliability. Homeland Security Presidential Directive 12 (HSPD-12) sets a clear goal to improve physical access control systems through the use of government-wide standards. The Federal Information Processing Standard 201 (FIPS 201) defines characteristics of an identity credential that can be interoperable government-wide. Smart cards support the implementation of these standards.

Smart cards usually look like a common credit card, although other forms are commercially available in the form of jewelry, such as a ring, pendant, or bracelet. The differences in appearance among the cards are aesthetic and are not related to the electronic features and functions available on the integrated circuits (IC) embedded in the plastic body of the cards.

The type of embedded IC determines the capabilities of a card. The two types of integrated circuits used in smart cards are microprocessor circuits and memory circuits. The capabilities of a microprocessor card are roughly equivalent to an early generation personal computer in terms of memory and processing speed; however, these capabilities are increasing with newer cards. Memory cards usually store minimal amounts of data, but such cards cannot perform data manipulations or computation, or execute processes, such as a collision resolution algorithm. The card reader must apply any encryption or changes to the data on a memory card. There are several memory configurations available, which allow certain sections of the onboard memory to be write-protected or reserved.

3.2.5.1 Operation

To operate a contact smart card system, a user must insert a card into a reader. The card reader provides power to the card, which causes the card to initialize. Depending on the type of card system, after initialization, the card can provide stored digital files such as biometric templates or encryption keys or perform algorithmic functions that have been defined by the security application programmers. Regardless of the system architecture, the card reader authenticates the card and then sends a message to the access control panel to open the entry point. A multitude of card readers are commercially available. Contact smart card readers often have built in numeric keypads for entering PINs and provisions for connecting biometric devices for two-factor authentication.

The mode of operation of the contact smart card provides some advantages to its use versus other access control technologies. First, because contact smart cards must be inserted into and withdrawn from a reader, as shown in Figure 3-13, the system throughput tends to be lower than for other smart card systems. Fumbling with the card and a delay during the initialization when the card comes into contact with the reader contribute to the lower throughput. Such a delay can be an advantage, because it provides the time required for touch-based and scan-based biometric authentication systems to work.

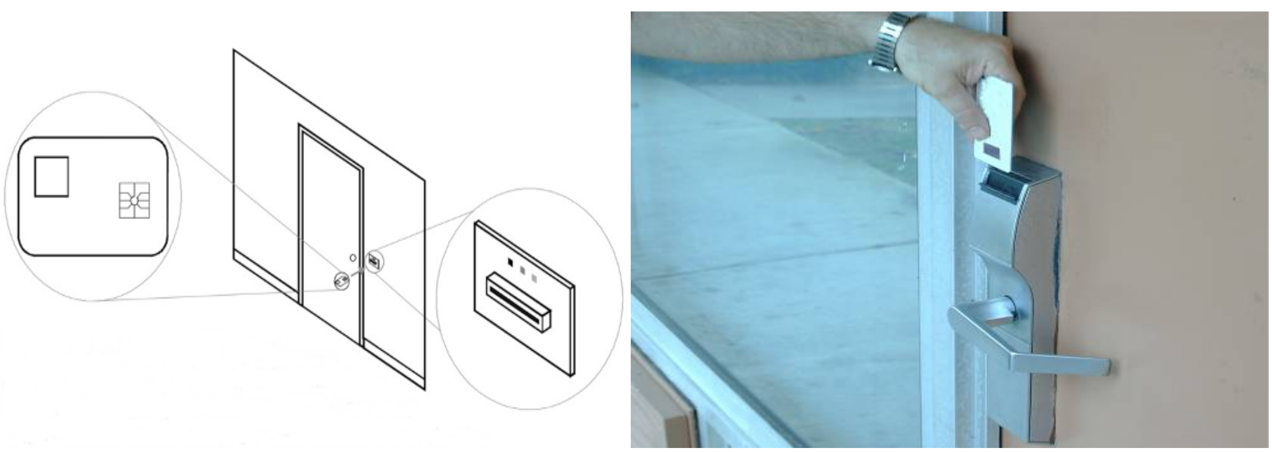


Figure 3-13. Contact Smart Card

3.2.5.2 Applications

Contact smart cards are suited for indoor, medium throughput access control systems where system flexibility is important. They are often used in high-security facilities and can handle large numbers of users.

Contact smart cards tend to be unsuitable for exterior applications because of the effects of weather on the contact points of the reader. Contact smart cards can be used for both physical and logical access control, as well as for tracking employee time and attendance. The overall value of the system can be increased by supporting other applications from the smart card platform. Besides providing secure identification and authentication, smart cards can be used as personal or organizational data holders and fiscal or accounting tools.

As a digital data storage device, the contact smart card has many potential applications. But when used specifically for access control, microprocessor smart cards offer many important advantages. The processor in the card enables the system manager to store the applications and computer programs on the card along with the data; magnetic stripe systems do not store enough information to have this capability. The advantage is that the applications and programs can be specifically tailored for the user’s access control requirements and can be changed as the need arises. For example, if a biometric system is used for authentication, managing several thousand templates using the facility’s central database and network can become an enormous task. Template management coupled with the multiple vulnerabilities associated with computer networking can disable the facility’s security program. Alternatively, the biometric template can be stored on the user’s smart card so that the template is always available when the card is presented to a reader. If the authentication algorithm is also stored on the card, then the card reader only needs to make the card run its own authentication program. The card responds after verifying the biometric, which is stored and processed on the card. The biometric template itself is more accessible and has a higher degree of security because the only time it is present in the facility’s system is during enrollment.

3.2.5.3 Performance Metrics

Performance depends on the specific technologies and applications used. The International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 7816 provides physical standards for contact smart cards, describing the size of the card, contact locations, electrical characteristics, and data transmission protocols. Proprietary cards and systems exist, particularly with memory only card systems. Transaction speed, as discussed in the contactless smart card technology review in Section 0, is a useful performance metric. The transaction speed of contact smart cards increases with higher processor speeds. Data collisions cannot occur because two cards cannot occupy the reader at the same time.

3.2.5.4 Vulnerabilities

Smart card systems that place authentication algorithms and templates on the cards and do not maintain online databases of this information are intrinsically more secure than systems that maintain online template databases. The only time a person’s template may be in the central network might be during enrollment for systems using card-based templates. Online template databases have some vulnerability to hacking.

There are a number of published procedures that detail methods to compromise the data on cards. Methods include dismounting the chip and using microscopic electrical probes to record the actions of the microprocessor; selectively erasing parts of the card's operating system to bypass or break encryption schemes; and operating the card outside of temperature, supply voltage, or external clock speed parameters to cause a software fault and generate a memory data dump. Normally, such assaults are cost prohibitive because the potential value of breaking the card is much less than the time invested. Tamper detection and protection are important issues and should be discussed with the card system vendor.

Punching holes in the card to attach a lanyard or a key chain can sever portions of the card's electronics and ruin it. Strong magnetic fields can scramble or erase the memory on some cards. Card holders should be instructed on the proper care of the card to reduce the incidence of these problems.

Overall, the vulnerability associated with the loss of a contact smartcard or a compromise of a PIN or password is less than that of many other systems. If the card is regularly used for entry, then a lost card will be promptly reported and can be quickly invalidated. Two-factor authentication makes personal information on a card more secure than information obtained from a stolen wallet or purse. The information is even more secure if the card has tamper resistant features in the circuitry or encryption. Finally, re-issuing a card is relatively simple, particularly if the issuing authority maintains an archive of card data.

3.2.6 Contactless Smart Card

Some access control systems use smart cards that, in addition to having processing or memory capabilities, have a radio frequency (RF) communications capability that allows a card reader to interact with them at a short distance. These are referred to as contactless smart cards. Contactless smart card systems can be used in high-security applications that may require greater throughput rates than contact smart card systems. Some smart cards can be equipped with magnetic stripes, barcodes, and other systems to facilitate access control.

Contactless smart cards resemble a common bank or credit card with an embedded microchip. Some vendors offer contactless smart devices in key fob or jewelry form. In key fobs and forms other than cards, the electronic components are often embedded in an epoxy resin rather than the plastic matrix used for cards. A contactless smart card must also have an antenna, which is embedded alongside the microchip.

A Combi Card is another type of RF capable smart card, which supports both the contact and contactless communication interfaces with a single microprocessor. The personal identity verification (PIV) card is an example of a Combi Card. FIPS 201 defines authentication mechanisms at three E-Authentication assurance levels (i.e., some, high, and very high confidence) and standardizes optional credential elements that extend trust in the PIV System to functions beyond authentication.

The ISO/IEC has defined standards for the characteristics of two general categories of RF capable smart cards.

- Proximity Card, 13.56 MHz ISO/IEC Standard 14443: Cards of this type are read-only and draw power from the card reader through inductive coupling. The reader range is 0 to 4 inches, depending on the specific brand of card and electronic elements supported. The bit transfer rate for proximity cards is 106 kilobits per second (kb/s). Cards of this standard represent the majority of contactless card deployments. There are two sub-types of proximity cards:
    - ISO 14443 Type A: The MIFARE® card uses lower cost memory and is primarily used for contactless ID applications. MIFARE is a proprietary series of chips that are used in proximity cards.
    - ISO 14443 Type B: This card offers a higher security microprocessor and encryption.
- Vicinity Card, 13.56 MHz, ISO/IEC 15693: Cards of this type offer longer operational range. These cards are often used for fare collection and inventory control tags. There are three modes of operation: read, authenticate, and write. The reader range varies by the mode used: read out to 25 inches, authenticate out to 20 inches, and write out to 15 inches. The bit transfer rate is 26.69 kb/s.

3.2.6.1 Operation

As an individual approaches the entrance to a controlled area, the contactless smart card enters the detection field of the card reader. Usually, the card bearer passes the card in front of the card reader at a distance of no more than 6 inches, but readers with ranges of up to 6 feet are available.

Some vendors recommend that the bearer tap the edge of the card on the face of the reader in order to keep the card in the reader field long enough to complete an authentication cycle. The size of the detection field varies, depending on the transmission frequencies and system’s communications protocols. In some systems, power is provided to the card from the detection field through the antenna. When the card is not in the detection field it is inert. Once powered, the card requires a very brief period for initialization. The card transmits the digital credentials to the card reader and if the individual is authorized the entry is unlocked.

3.2.6.2 Applications

Hands-free operation of contactless smart card systems minimizes the time spent at a physical access portal. This is an advantage for those workers carrying goods and materials into the workspace. Hands-free operation is also a requirement often associated with systems that operate at high levels of throughput, such as large public buildings or sports venues, where large numbers of people pass through access portals within a brief period of time. If high levels of throughput are required, caution should be used when selecting an appropriate technology for two-factor authentication. Some contactless card readers often have built in numeric keypads for entering PINs, as shown in Figure 3-14, and provisions for connecting biometric devices for two-factor authentication. Contactless smart cards are best suited to applications where tracking personnel and materials inside a protected area are required. This technology can be used for both interior and exterior applications.

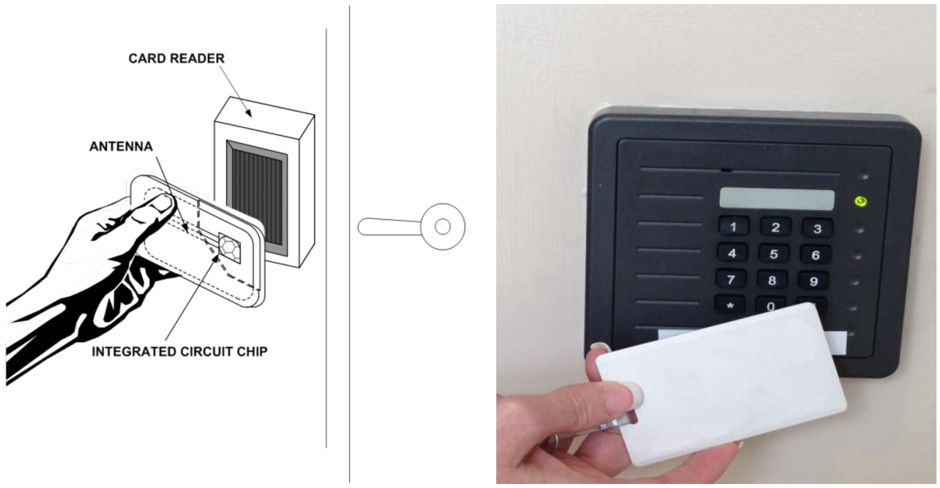


Figure 3-14. Contactless Smart Card

3.2.6.3 Performance Metrics

Performance depends on the system's specific technologies and applications. The general measures of contactless smart card performance include the transaction speed, read range, and the anti-collision techniques used.

The transaction speed is the total time required to complete the assigned function. A transaction cycle has four steps: input/output (I/O), memory access, encryption, and processing. Benchmark transaction speed metrics can be misleading, particularly if one part of the cycle is heavily stressed over another. For example, an access control application may only need to send a few bytes of information in order to authenticate. In this case the I/O function may be under-stressed compared to the encryption or processing steps. Another application could require transmitting several hundred bytes to provide a biometric template to a reader, stressing the I/O subsystems and leaving the processing step underutilized. The transaction speed metric must be considered in the full context of the system's use.

Read range should also be considered within the context of the intended application. The read range is the maximum distance between the card and the reader where a transaction can be successful. The primary factor affecting read range is the power requirement of the card. Cards with microprocessors use more power than memory-only cards and require a shorter read range. The strength of the reader field is another factor. There will also be some variation in the power requirements between identical cards from the same manufacturer.

A collision occurs when a card reader sends out a request for data transfer and two or more cards respond at the same time. Anti-collision techniques refer to the methods used to resolve collisions and return coherent messages to the reader from the cards in the field. The speed at which the system can resolve collisions is a significant factor in the system's overall performance. Collisions occur more frequently with longer read ranges and longer transaction times.

The two techniques below, which are commonly used, require the card to have an on-board processor.

- Bit Collision Technique—when a collision is detected because the reader received unintelligible bits, the reader ignores the response and uses software techniques to restrict subsequent requests for data transfer until only one card responds. Since the read range for this type of card is only 4 inches, collisions will not be a major issue. ISO/IEC 14443 is the primary contactless smart card standard being used for transit, financial, and access control applications. It is also used in electronic passports and in the FIPS 201 PIV.
- Slot Marker Technique—this technique requires the card reader, when idle, to send continuous request messages within a specific time slot to find cards in the vicinity. ISO/IEC 15693 establishes standards for the physical characteristics, radio frequency power and signal interface, and anti-collision and transmission protocol for vicinity cards that operate to a maximum of 1 meter (i.e., approximately 3.3 feet).

3.2.6.4 Vulnerabilities

Contactless smart card systems that place authentication algorithms and templates on the cards are intrinsically more secure than systems that maintain this information online. Once online this information can be stored in central archives offline. Online template databases always have some vulnerability to hacking. Other vulnerabilities are similar to the contact smart cards discussed in Section 3.2.5.4.

3.2.7 Wiegand Cards

A Wiegand card is a plastic or vinyl credit-card sized device that contains two rows of small parallel wires of proprietary composition that generate a binary number when the card is passed through a reader. The wires are embedded within the card during the manufacturing process and provide protection against forgery. Outside the reader’s magnetic field, the embedded wires are essentially inert.

Wiegand access control systems were developed in the early 1970s and used throughout the public and private sectors. However, many Wiegand access control systems are aging and require frequent maintenance. The Wiegand card is largely being replaced by the smart card.

3.2.8 Key Fobs

Key fobs are used as interface devices to many access control and security systems (Figure 3-15). Several of the technologies discussed in other sections of this handbook are available in key fob configurations. They can be made of plastic, epoxy resin, or metal.



Figure 3-15. Key Fob

3.2.8.1 Operation

Depending on the system that it controls, key fobs can operate by a number of different methods. Garage door openers, facility alarm controllers, and fobs used in the automotive and transportation industries transmit a coded radio frequency identification (RFID) signal to a receiver inside the vehicle or facility when the operator presses an

appropriate key or button. Key fobs using RF transmissions are usually made of plastic or epoxy to avoid interference with the transmitted signal. The radio signal contains a binary number that is a control code. Encrypting the transmitted signal can enhance the security of the system.

3.2.8.2 Applications

The key fob interface is flexible and is an element of many access control and security systems. For example, a household garage door opener provides a basic access control system for many homeowners. Such systems range in complexity from simply producing a loud alarm to systems with satellite communications, global positioning system (GPS) location, and remote disablement of a vehicle to prevent theft or other criminal activity. Key fobs that control facility alarm systems often have a small keypad with three or four buttons. Each button on the keypad controls a state of the alarm system, such as arm or disarm. Key fobs used in facility alarm systems often include a duress alarm or a panic button that can trigger an alarm independently of the state of the system and sensors. The key fob interface is suitable for both interior and exterior applications, and is particularly useful in vehicle and transportation industry applications.

3.2.8.3 Performance Metrics

The performance of key fob interfaces depends on the systems with which they interact. Key fobs that use radio frequency transmissions will eventually require the battery or the whole fob to be replaced. The range at which such systems operate is also a quantifiable consideration in the overall system design.

3.2.8.4 Vulnerabilities

Theft is the main vulnerability for key fobs. Two-factor authentication, using a PIN or biometric access control, can significantly reduce the vulnerability of the entire access control system if a key fob is lost or stolen.

3.3 Biometric Access Control Technologies

Biometric access control refers to the use of human biological attributes for verification or identification in physical access control systems. Biometric systems use physical or behavioral data measurements to compare with previously enrolled information to determine such system responses as establishing identity or granting access. Biometric access control systems are built around some of the measurable attributes listed in Table 3-1.

Table 3-1. Biometric Attributes Used in Access Control Systems

Biometric	Physical	Behavioral
Facial Recognition	✓	
Fingerprint Recognition	✓	
Hand/Finger Geometry Recognition	✓	
Vein Geometry Recognition	✓	
Iris Recognition	✓	
Voice Recognition	✓	✓
Signature Dynamics Recognition		✓

Most biometric access control systems feature the following:

- Physical characteristics include the anatomical components and physiological functioning of the human body, while behavioral characteristics describe the way an individual reacts or moves within the environment.
- Biometric access control systems can be automated so that they work without direct human intervention. They generally produce an access control decision in a few seconds or less.
- A human physical and/or behavioral characteristic can be used as a biometric identifier if it meets certain tests:
  - Universality: most people should possess it
  - Unique: any two persons should always exhibit different versions of the same characteristic
  - Collectability: the characteristic must be easily and quickly measurable
  - Permanence: the biometric measurement should be stable over a long period of time.

3.3.1 Devices

Biometric access control devices extract measurements of the characteristic of interest, construct a mathematical template from those measurements, and compare it to the reference record in an enrollment database to control access. This process is typically referred to as feature extraction. Privacy concerns are minimized because the biometric parameter that was measured cannot be recreated from the template data. For example, it is impossible to reconstruct the fingerprint image from the template derived from a fingerprint scan.

The reader uses a predetermined number of points on the fingerprint and converts that information to binary data using mathematical computations. This creates a sample template.

The system compares this template to a database of fingerprint reference records and either finds or fails to find a corresponding record that identifies the subject. Once the data is located or determined not to exist, the system processes this information accordingly. Some systems may retain fingerprint images in an enrollment archive for retrieval.

3.3.2 Verification and Identification

In access control security applications, biometric systems can be used for verification or identification. Biometric systems enhance the access control verification and identification processes by capturing characteristics of individuals, extracting measurable features, and comparing the data against enrolled biometric records. Unlike passwords or PINs, the enrolled biometric template cannot be shared or stolen; therefore, positive verification or identification can be assured within the limits of the biometric system's capability.

Verification, sometimes referred to as one-to-one matching, determines if a person is whom he or she claims to be. This process involves capturing a person's biometric data and matching it against an existing record for that person. Verification requires a claimed identity typically using a token or a PIN. Biometric systems automate the verification process by capturing characteristics of individuals, extracting measurable features from them, and comparing the data against the enrolled record associated with the claimed identity. If the match score meets the decision threshold, access is allowed. Otherwise, access is denied. Verification is often used in access control systems where multifactor authentication is required.

Identification, sometimes referred to as one-to-many matching, determines who an individual is. The identification process would be used in situations when no credential or PIN is required to be presented to the access control system. With this process, a record of a person may be known to exist in the database (i.e., closed-set identification) or may not be known to exist in the database (i.e., open-set identification). His or her biometric data is compared against all existing records in a database in order to find a match. If a match is found and meets the decision threshold, access is allowed. Otherwise, access is denied. Identification is typically used in low security applications.

3.3.3 Performance Metrics

There are four primary metrics associated with the performance of biometric systems. These are the failure to enroll (FTE) rate, false match rate (FMR), false non-match rate (FNMR), and the equal error rate (EER).

The FTE is the probability that a user will be unable to enroll in a biometric system due to insufficiently distinctive biometric sample(s). Users incapable of providing biometric data, such as amputees, are normally not counted in a system's FTE rate. This rate varies with the type of biometric. Some types of biometric access control systems are more susceptible to enrollment problems and each manufacturer deals with the problem in unique ways.

The FMR is the probability that a system will confuse two different individuals. That is, an access control system may allow an unauthorized individual to pass. This rate must be extremely low for a system to be considered usable. In most biometric security systems, FMRs range between 0.00001 and 0.1 percent. FMR is also known as false acceptance rate (FAR) in some access control systems.

The FNMR is the probability that an individual's data will not be matched to corresponding data in the access control system database. That is, the system will deny access to a person who should be authorized to enter a protected space. This rate is also kept as low as possible to prevent users becoming frustrated with the system. Biometric system FNMRs range between 0.000066 and 1.0 percent. FNMR is called false rejection rate (FRR) in some access control systems.

One method of measuring overall performance of a biometric system is by looking at the EER. The EER is defined as the point on a graph where the FMR and FNMR intersect. That is, the same numbers of errors of both types (FMR and FNMR) are made. The smaller the EER, the more accurate the biometric system is.

Depending on the application and the system selected, each of these metrics may be more or less important in the security scenario. For example, just because biometric system A has a lower score in FNMR than system B does not mean that for every application A is better than B.

3.3.4 Threshold Adjustments

The effectiveness of the system is partially a function of its ease of use as well as its sensitivity. Users prefer systems that are convenient, easy to work with, and reliable. On the other hand, security considerations dictate that the system should never allow unauthorized persons to gain access. At times, these are mutually exclusive concepts. Biometric access control system sensitivity can be adjusted to favor security or convenience, as shown in Figure 3-16. Since biometric systems are probabilistic, the allowable variation from exact conformance to the enrolled pattern is adjustable.

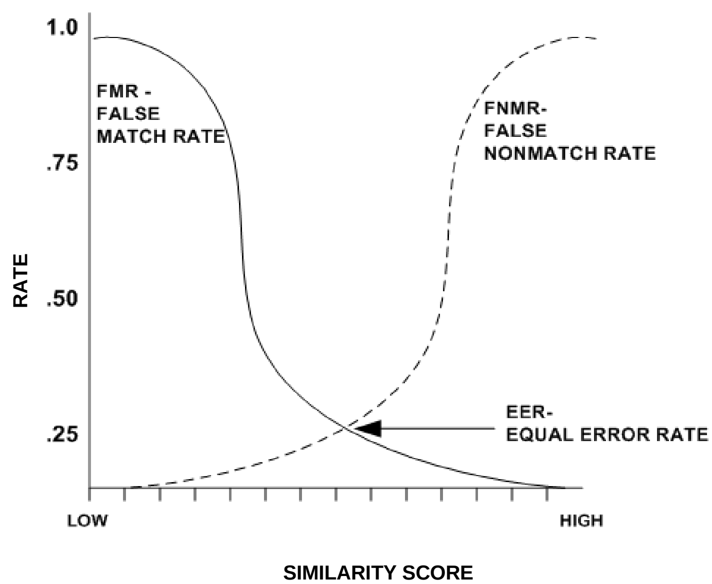


Figure 3-16. Security Threshold Adjustment

3.3.5 Operation

A user's biometric data is collected in a process called enrollment to create a reference template. Enrollment is the process by which the biometric data of individuals is captured and stored so that it can be used for matching at a later date. A verification system, for example, could require the creation of a relatively small biometric database containing records on all personnel authorized to access a particular facility. An identification system, however, must query a much larger database, or set of databases, to identify the user against all others in the system.

Depending on the configuration of the system, the reference may either be stored within the system or stored electronically on a card or other type of token carried by the user. When the user attempts access, the system captures a biometric sample and unique features of the sample are extracted and analyzed. The results are then compared to the reference template in the enrollment database. If a match is found within a certain level of tolerance, access is granted; if not, access is denied.

3.3.6 Facial Recognition

Facial recognition is a biometric access control technology that uses one or more photographic images to recognize a person by measuring points on a face under controlled conditions. Facial recognition systems are not intrusive, require no physical contact with the user, and have a high rate of user acceptance.

Facial recognition is not affected by race or gender-based differences in appearance. It is a robust technology capable of handling a wide range of body types and facial characteristics. Facial recognition is used throughout the world in industries as diverse as banking, gaming, healthcare, law enforcement, customs, and retail. The technology has been tested successfully in neutral industry comparisons and is currently the fastest growing segment of the biometric access control market.

Facial recognition has a number of desirable aspects.

- The process is intuitive. The user's interaction with the camera is similar to being photographed for any number of identification applications, from driver's licenses to passports.
- Facial recognition is non-intrusive. Unlike other biometric access control systems, facial recognition requires minimal interaction with the user.
- Facial recognition is hands-free. The user makes no physical contact with the camera, or detector, and does not contaminate it with body oils or other debris.
- Facial recognition systems retain a photographic record of attempted entries by unauthorized personnel. Although some fingerprint systems can store the fingerprint of an unauthorized user, fingerprint analysis requires special training. Analyzing and recognizing faces is a natural, instinctive human behavior.
- Finally, ambient lighting is sufficient for most facial recognition applications, with no requirement for special white or infrared lighting. However, matching is most effective when the ambient lighting is similar to the lighting used to create the template during enrollment.

3.3.6.1 Operation

A number of technologies are used in facial recognition access control systems. The two major categories are video imaging and thermal imaging. Video facial recognition analyzes the unique shape, pattern, and positioning of facial features by mapping those features to create a mathematical model (Figure 3-17). Video can be further subdivided into two-dimensional (2-D) and three-dimensional (3-D) imaging. The number of cameras used is the primary physical difference between the systems.

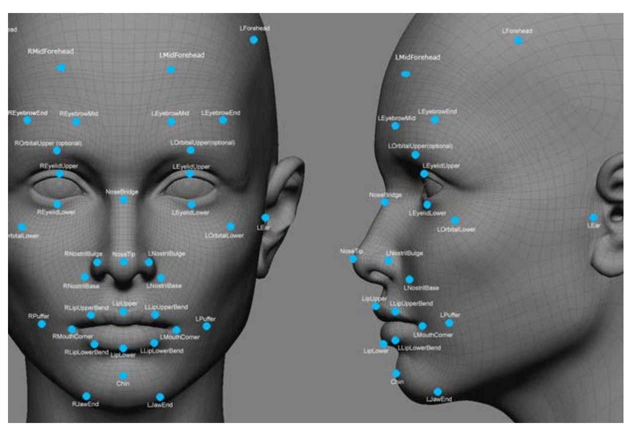


Figure 3-17. 3-D Facial Recognition

3-D systems use two cameras and integrate the images to create a 3-D digital template. In 2-D models, a single camera acquires the image. Thermal imaging uses an infrared camera to produce a facial thermograph. The system digitizes the thermal pattern resulting from the heat produced by the blood vessels under the skin.

Facial recognition enrollment for access control purposes is straightforward, requiring 20 to 30 seconds to take several pictures of the enrollee's face. This photographic sequence is best done with varying angles and expressions to allow for more accurate matching. The system extracts the relevant information and uses mathematical techniques to create a reference template that is stored in the database.

Verification is similar to enrollment. The user claims an identity through a login name, smart card, or terminal entry and then sits or stands in front of the camera for a few seconds. The system captures an image, creates a template from the extracted information, compares it to the reference template, and then grants or denies access. The point at which the two templates are similar enough to match, known as the threshold value, can be adjusted for different persons, time of day, and other factors.

3.3.6.2 Applications

Facial recognition is useful for indoor verification applications where the ambient lighting and environment can be controlled. The camera must be situated so that quality facial images can be captured. Facial recognition is not recommended for areas where lighting is not uniform or situations where personnel protective equipment (PPE), such as face masks, is required.

3.3.6.3 Performance Metrics

The most obvious and useful metric for facial recognition access control is the quality of the capture device. In general, the greater the resolution and contrast of the captured image, the better the system will recognize faces. Processing time is an important factor in user acceptance. A system should be able to discriminate a live face from attempts to spoof, or deceive, the system using a photograph or a video feed. Finally, any access control system should have a low FMR.

The reliability of some facial recognition systems can be affected by one or more factors involving the user or the environment. Differences in the devices or the light conditions in the enrollment and field environments can increase the false rejection rates. Changes in facial hair, hairstyle, headgear, eyeglasses, body weight, or facial aspect (e.g., angle at which the image is captured) can change the facial shape or outline. Loud or bright clothing can interfere with the system's ability to distinguish the face in the image. Too much or too little movement on the part of the user can cause some systems to reject falsely or to fail to recognize a live face.

3.3.6.4 Vulnerabilities

Some 2-D facial recognition systems may recognize photographs or video material as a face and allow access to an unauthorized person. Systems that are 3-D are not as vulnerable to spoofing. Recent 2-D systems are capable of recognizing live faces and are not vulnerable to photo or video induced false matches.

3.3.7 Fingerprint Recognition

Fingerprint recognition is one of the most widely used biometrics in the access control industry. This is because fingerprints are one of the oldest forms of personal identification, inexpensive to collect and analyze, and they are stable. Biometric fingerprint access control applications use one or both of two fingerprint characteristics: ridge patterns and minutiae details, which are unique features found within the patterns. Some extremely hi-tech biometric fingerprint scanners not only require a fingerprint to match, but they employ temperature and humidity monitors to ensure that a live finger is being scanned.

There are three basic patterns, as seen in Figure 3-18, of fingerprint ridges: the arch, loop, and whorl.

- The arch is made up of ridges lying one above the other in a general arching formation.
- The loop is made up of ridges that enter from one side of the finger, form a curve, and then exit on the same side.
- The whorl is made up of ridges that form a circular pattern around a central point.



Arch **Loop** **Whorl**

Figure 3-18. Fingerprint Patterns

Minutiae recognition, as seen in Figure 3-19, is the most common form of biometric access control fingerprint identification. Minutiae include the discontinuities that interrupt the otherwise smooth flow of fingerprint ridges and the abrupt ridge endings and bifurcations. The major minutia features of fingerprints are bifurcation, dots, and ridge endings.

- Bifurcations are the points where one ridge divides into another.
- Dots are very small ridges, no longer than the width of adjacent ridges.
- Ridge ending is the point where a ridge terminates.

The ridge patterns and minutiae are important in fingerprint analysis since no two fingerprints are identical.

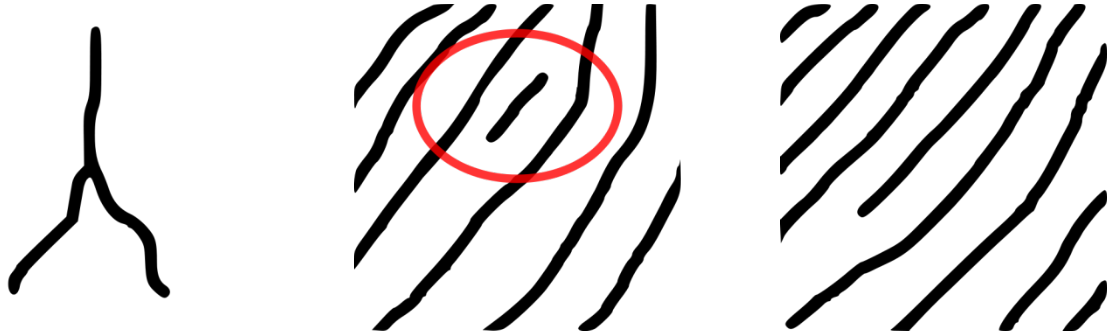


Figure 3-19. Fingerprint Minutiae

3.3.7.1 Operation

A fingerprint sensor is a device used to capture a digital image of a fingerprint. There are several commercially available sensor technologies for electronically collecting fingerprints, including optical, silicon, ultrasound, and light emitting.

Optical technology is the oldest and most widely used collection method. For optical collection, the finger is placed on a proprietary, coated platen. A charged coupled device (CCD) converts the image of the fingerprint, dark ridges and light valleys, into a digital format. Optical devices can withstand temperature fluctuations, are inexpensive, and provide resolution typically ranging from 500 to 1,000 dots per inch (dpi). Drawbacks of optical technology primarily relate to the requirement to make contact with the reading device's surface. Users leave residual fingerprints, grease, dirt, and other materials that interfere with the reader's performance and cause the reading surface to wear. Some of the new contactless optical fingerprinting detectors eliminate these deficiencies.

Silicon chip technology, or capacitance technology, has gained considerable acceptance since its introduction to the marketplace in the 1990s. In most chip systems, the sensor acts as one plate of a capacitor and the finger acts as the other. The capacitance between the detector and the finger is converted into an 8-bit grayscale digital image. Silicon generally produces better image quality with less surface area than optical technology. Silicon-based equipment can be much smaller than optical devices. The primary drawbacks are a shorter track record for durability in suboptimal environments compared to optical technology, the smaller scanning surfaces, and issues relating to the requirement to touch the reader's surface.

Ultrasound technology has only recently been introduced to the biometric market, thus it is not widely used. Ultrasound uses high frequency sound waves to measure the impedance of the finger, air, and platen to generate a signal. Sound waves penetrate the dirt, grease, and other contaminates to obtain an image of the tissue and veins of the finger. This process can obtain usable prints in some situations that would impede optical systems. Some systems can resolve fingerprints of small children, petite adults, and persons with dry, rough, or worn fingers that can be difficult for other systems. Systems can also differentiate between dead skin and live skin. The technology's main drawback is its newness in the market and lack of a track record.

Light emitting sensor technology uses electroluminescence film on its sensors. When a finger is in contact with the film and an electric field is applied, a high resolution image of a fingerprint is produced. The film is durable, works in direct sunlight, and is very lightweight, making it easily adaptable for mobile applications.

Regardless of the technology applied, there are several steps required to convert a high-quality captured print into a compact template. Feature extraction, as this process is called, is the basis by which fingerprint technology produces a usable sample. The exact processes used are proprietary to each access control vendor. As shown in Figure 3-20, the user places a finger or fingers on the reader. The reader captures the image and then, based on its design, will use complex algorithms to characterize the print for comparison to the template in the access control database.

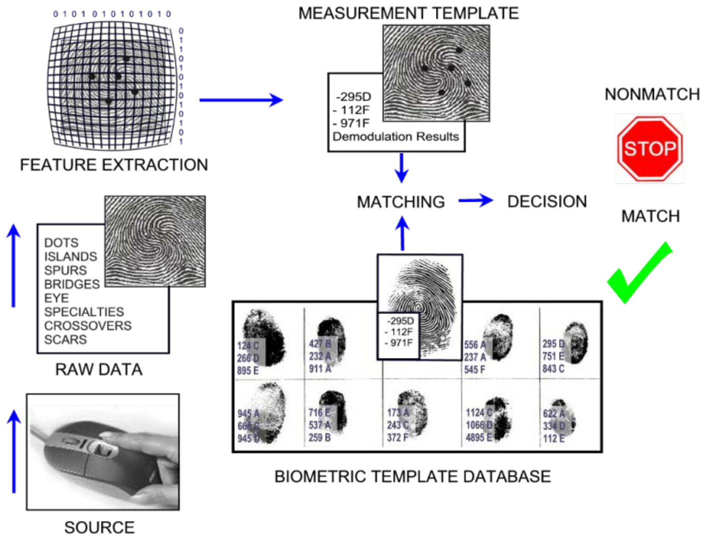


Figure 3-20. Fingerprint Recognition

Fingerprint scanning technology continues to advance in multiple ways, including image capture unaffected by lighting environment, spoofing detection of fake fingerprints, and liveness detection. Liveness detection ensures a pulse is associated with the captured fingerprint sample to prevent the exploitative use of dismembered digits or fake digits. Also, highly detailed 3-D representations of finger surfaces and contactless live scan devices are being developed that produce prints of fingers, and in some cases, the entire hand, from a standoff position.

3.3.7.2 Applications

Fingerprint-based access control systems are used for both identification and verification purposes. The technology is mature and available from a variety of vendor sources. Silicon chip and light emitting sensor based systems can be small enough to use with mobile devices, such as smartphones, tablets, or laptop computers.

Fingerprint-based access control systems are for indoor/outdoor use and respond well to a wide range of environmental humidity and temperature conditions.

These systems are not recommended for applications in which users wear gloves or work in conditions that cause abrasion to the fingers and hands. Such applications might include construction sites, nuclear/chemical surface contamination areas, or foundries.

3.3.7.3 Performance Metrics

The most fundamental feature of a reader is the size of the scanner's sensing area. The average size of a fingerprint is approximately 0.5 by 0.7 inches (smaller for children and females, larger for males). A smaller reader surface obtains a partial print, which may not include all of the area required for enrollment scans. Smaller reader surfaces render the system more sensitive to differences in finger positioning for each reading and may result in unacceptable false rejection rates. Optical and ultrasound systems are more likely to have larger sensing areas than chip systems, because large chips that perform uniformly over the entire surface are difficult and expensive to make. The sensing area of a chip system is dependent on the size of the chip.

Rates of failure to enroll can be high for some systems when the user population includes children, petite adults, or persons with finger surfaces that are worn, rough, or dry. Recent technologies claim to have improved performance for these difficult categories.

Another important parameter is the number of pixels characterizing an image (i.e., resolution). A minimum image resolution of 500 dpi is required by FBI-compliant systems. To capture minutiae requires a minimum of 250 to 300 dpi. Resolutions higher than 500 dpi may be necessary to enroll children and petite adults whose print characteristics are too small and close for some systems to read.

Finger placement is very important in order to obtain an accurate and repeatable print. Other parameters of importance include the cleanliness of the finger, the contrast, and the amount of geometric distortion present in the sample. Systems that require contact with the reading surface require relatively frequent cleaning to remove latent prints and maintain high sensing accuracy.

3.3.7.4 Vulnerabilities

Some fingerprint systems may be vulnerable to spoofing using 3-D molds of an enrollee's fingerprint. Technology to verify that a finger is live is available in some systems to reduce the likelihood of spoofing.

3.3.8 Hand/Finger Geometry Recognition

Hand geometry recognition systems are commonly available in two forms: full hand geometry systems that measure the entire hand, and finger geometry systems that measure only the index and middle fingers. Hand and finger geometry biometrics are automated measurements of hand and finger dimensions taken from a three dimensional image. A reader or camera captures up to 96 features of the hand such as the shape, width, length of fingers and knuckles, distance between joints, and the shape and thickness of the palm. This is similar to some types of facial recognition systems in that it examines the spatial geometry of the hand and fingers. Surface details such as fingerprints, lines, scars, dirt, and fingernails are ignored.

Now a mature technology, hand geometry was one of the first methods of biometric access control in the modern marketplace. Unlike other biometric access control systems, which have taken advantage of such technological breakthroughs as microchips or increased camera quality, the technology supporting hand geometry access control systems has not progressed significantly for many years. Hand geometry access control systems have been in use for almost 30 years at facilities that include nuclear power plants, welfare centers, immigration facilities, and day care centers.

3.3.8.1 Operation

Capturing a hand or finger geometry sample is straightforward, as shown in Figure 3-21. For hand geometry, the enrollee places their hand, palm down, in a detector containing a flat plate with five pins that guide the placement of the fingers. The detector registers the dimensions of the hand and fingers using an LED, a camera, and mirrors. Typically, three placements are required to enroll, and the enrollment template is a representation of the average of the measurements from the three placements.

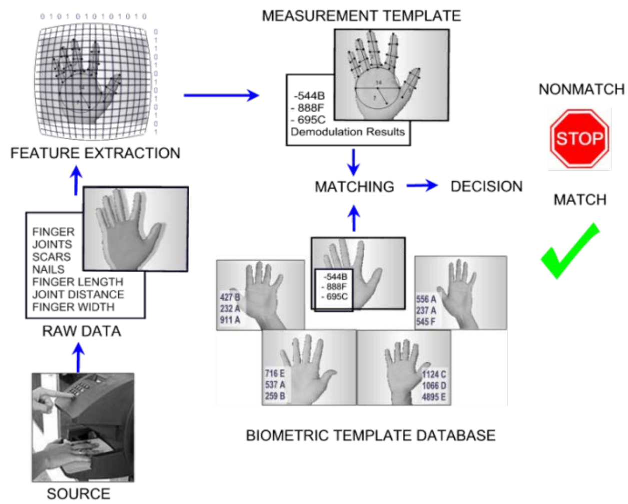


Figure 3-21. Hand or Finger Geometry Recognition

3.3.8.2 Applications

Hand geometry is a relatively accurate technology, but it draws upon less data points than fingerprint, iris, or facial recognition. Hand geometry is quite useful in verification, such as matching a known user to that user's enrollment template. The factor limiting hand and finger geometry to verification applications is that hands and fingers do not vary enough in dimensions to generate unique templates in large populations of users. Within the acceptance tolerances of the detector, each time a user seeks access, the data for more than one enrollee could generate a match. Therefore, an identification process, such as using a PIN, fingerprint, smart card reader, or some other device, should accompany hand geometry systems.

Hand geometry access control systems are especially useful in outdoor environments because the detectors are resistant to many environmental factors, such as ambient lighting or temperature changes. Hand geometry templates are small, making them portable and enabling the entire control system to be contained in a single detector unit. Since dirty or soiled hands do not affect hand geometry access control devices, these systems can be used at construction sites and foundries.

3.3.8.3 Performance Metrics

System operation is comparatively fast for access control. Access authorization typically takes place in two to three seconds. Throughput can be up to 10 users per minute.

Hand geometry FTE rates are low compared to some other biometric systems. FTE rates measure the likelihood that a user is incapable of enrolling in the system. Fingerprint recognition, for example, is prone to elevated FTE rates because of poor quality fingerprints, and facial recognition requires consistent lighting to enroll a user. Hand geometry does not suffer from such operational or environmental constraints. Hand geometry can have higher FMR rates making it more suitable for verification than identification. Since most users can use hand geometry for access control, few employees and visitors need to be processed outside the system.

3.3.8.4 Vulnerabilities

The primary vulnerability of hand/finger geometry systems is the probability that more than one person's hand/finger geometry sample meets the threshold criteria for a match with a template is significantly greater than most other biometric systems. This also makes hand geometry more vulnerable to spoofing attacks.

Some situations involving a user can result in false rejections. Swelling or injury to the hand, the presence of bandages or jewelry, and changes in weight that affect the dimensions of the hand can result in false readings. Incorrect placement of the hand can also result in inaccurate measurement.

3.3.9 Vascular Pattern Recognition

Vascular pattern recognition access control systems use the patterns formed by veins on certain parts of the body, such as the back of a hand, finger, wrist, or face. These systems can be used for identification and verification. Vascular pattern recognition is a relatively new technology within the biometric access control industry and uses miniaturized infrared scanning technologies. Although these systems are less mature and may be more costly than other access control technologies, the maturity of vascular pattern recognition is increasing.

3.3.9.1 Operation

An infrared camera used as a scanner can detect the pattern of veins located directly under the skin. These patterns are unique to an individual and do not vary over a person's life.

During enrollment, a user positions the required skin area over the scanner opening while the scanner makes several infrared pictures, as shown in Figure 3-22. The system produces grayscale images of the infrared pictures, which are converted to binary representations. Algorithms extract the useful features from the binary pictures and render them as a mathematical pattern or reference record, for matching during later verifications.

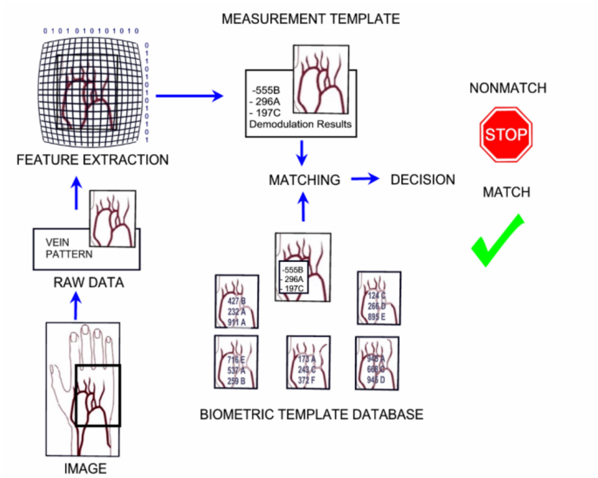


Figure 3-22. Vascular Pattern Recognition

To gain access, the user's vein sample is taken. The system then computes a template and compares it to the reference templates generated during enrollment. The system grants access if the template meets the criteria of a match.

3.3.9.2 Applications

Vascular pattern recognition systems can be used in high-security access control situations requiring identification or verification. They can be programmed to read body areas other than hands when many employees' hands might be otherwise occupied. Vascular recognition technology is widely deployed at ATMs in Japan.

3.3.9.3 Performance Metrics

Manufacturers claim a 99.98 percent enrollment rate, one of the highest rates in the biometric device industry. Users accept this type of biometric because it is non-intrusive, requires minimal contact with the skin, and takes less than one second to return a result even on large systems with several thousand registered users. Since these systems are relatively new to the market, they lack the long-term performance track records of older, more mature technologies.

3.3.9.4 Vulnerabilities

Few vulnerabilities are associated with vascular pattern recognition systems. The operating principle behind these systems relies on blood flow through the veins. It is nearly impossible to defeat a properly functioning system.

3.3.10 Iris Recognition

The iris recognition system takes an infrared picture of the iris from a distance of 4 inches to 6 feet. This is considered by users to be non-intrusive. The iris is the plainly visible, colored ring that surrounds the pupil. It is a muscular structure that controls the amount of light entering the eye. The iris is composed of measurable intricate details called striations, pits, and furrows. No two irises are alike; even a person's two irises are completely different. The quantity of unique information that can be measured in a single iris is much greater than in fingerprints.

Iris recognition technology has traditionally been deployed in high-security situations when imaging can be done at a distance of less than three feet, and there is a need to search very large databases without incurring false matches. These systems are in use in a number of high profile applications, including airline passenger screening, prisoner recognition, and physical access to healthcare records. Iris recognition systems are:

- Stable—the human iris remains stable over the course of a person's entire lifetime. This makes iris recognition a very desirable biometric for access control uses.
- Unique—iris recognition is widely regarded as the most accurate biometric methodology due to the rich level of detail that can be gathered. Available systems capture over 240 unique characteristics in formulating the template, which is over 10 times as much as other biometric systems. The probability of two irises having the same pattern is essentially zero.
- Flexible—unlike some other biometric access control systems, iris recognition requires no physical contact. This means it is ideally suited for use in environments where gloves or other protective gear is used. Iris recognition technology can integrate easily into existing access control systems or operate as a stand-alone system.
- Reliable—since the system uses infrared images, only a live iris can register. The distinctive iris pattern is not susceptible to theft, loss, or duplication. The illegal use of an iris pattern from an authorized user is unlikely and models of the iris that can fool the detector are almost impossible to produce. At death, iris tissue is one of the first body tissues to deteriorate; forensic pathologists use the iris as an accurate estimator of the time of death. This prevents spoofing the system using an eye removed from an authorized user.

- Non-Intrusive—although the term “iris scanning” is often used in reference to iris recognition technology, there is no scanning involved. Iris recognition uses a camera to capture an image of the iris and then converts that image into a template. No bright lights or lasers are used in the imaging process. Glasses and most contact lenses can be worn during the procedure without compromising the system’s accuracy.

3.3.10.1 Operation

In 1993, Dr. John Daugman, Ph.D., Cambridge University, England, first described the process for obtaining and processing iris images using near infrared (NIR) light to identify the patterns present in the iris not normally seen with visible light.

Daugman’s process uses a dedicated monochrome CCD camera no more than 3 feet from the eye using both visible and infrared light. The frequency range of infrared light (i.e., 700 nanometers [NM] to 900 nm) is the same range used by ophthalmologists to study macular cysts and is harmless to the eye. The LEDs used to produce this light are similar to those used in television remote controls, toys, and other consumer products. The energy entering the eye is much less than when a person stands in sunlight or looks at an incandescent lamp.

Various factors can affect an image of the iris including the camera angle, size of the pupil, angle of the head, or direction of the eye position. Vendors use mathematical methods to compensate for these factors.

The core of the iris recognition system (Figure 3-23) is the software that performs the following functions:

- Acquires the image of the eye including the iris.
- Defines the boundaries of the iris. The software narrows the image in from the right and left periphery to locate the outer edge of the iris. This horizontal approach accounts for the obstruction caused by the eyelids. At the same time, it locates the pupil (inner edge of the iris) and excludes the lower 90 degree cone of the iris due to inherent moisture and lighting issues.
- Establishes a polar coordinate system over the iris.
- Defines zones for analysis within the coordinate system. Some filters span as much as 70 percent of the iris, but most use less. The images provide exceptional detail, well beyond what a pictorial or point-based representation could provide.
- Analyzes image data by converting it into complex mathematical expressions in a process called demodulation. The algorithms filter and map the segments of the eye into hundreds of vectors similar to a DNA sequence code. These vectors define “the what” and “the where” of the sub-image.
- Generates a template. At this point the database will not be comparing images of the iris, but rather hexadecimal representations of data returned by the demodulation process.
- Stores and often encrypts the template.
- Matches the user’s access request template to the enrollment template to grant or deny access.

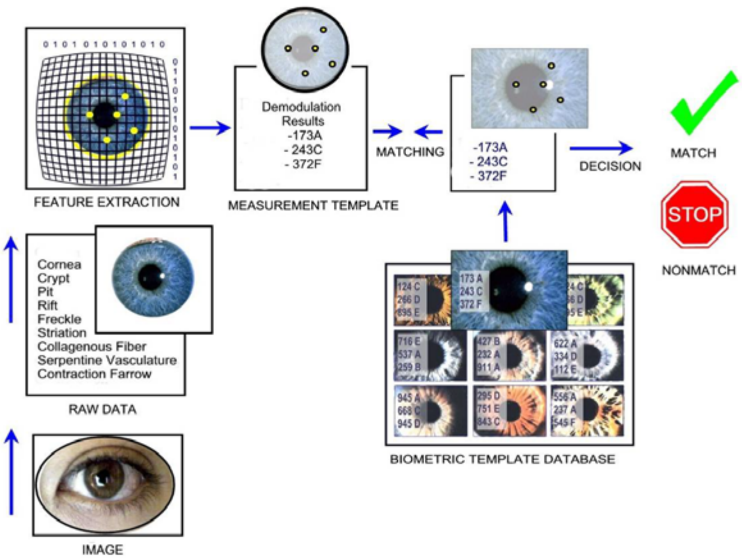


Figure 3-23. Iris Recognition

3.3.10.2 Applications

Iris recognition access control is highly accurate and is a good choice for high-security applications. Iris recognition can be used for identification and verification tasks. Prisoner verification is one of the common uses of iris recognition in law enforcement. Additionally, the FBI is adding iris recognition to its national biometric database.

3.3.10.3 Performance Metrics

The minimum imaging system resolution to capture the rich details of the iris pattern requires at least 50 pixels in the iris radius. Most commercial systems capture from 100 to 140 pixels.

Most software vendors advertise speeds of over 500,000 image matches per second. Overall, system cycle times from the initial reading to access should be a few seconds for a standalone iris recognition device. Manufacturers' claims for accuracy may overstate the actual capability of the technology. Most EER measures are derived from assessment and matching ideal iris images.

3.3.10.4 Vulnerabilities

Iris recognition technology requires a reasonably controlled and cooperative user. Traditionally the enrollee must remain still for a moment in a certain spot; however, emerging technology is able to capture the iris without requiring the person to remain still. Many users struggle to interact with the system until they become accustomed to its operation; however, like other biometric modalities, as a person becomes more familiar with the system false rejections decrease.

Image matches depend on the quality of the image. A poor quality enrollment can make later matches more difficult.

3.3.11 Retina Scan

The retina is a thin nerve (1/50 of an inch) on the back of the eye. It is the part of the eye that senses light and sends impulses through the optic nerve to the brain. It is the rough biological equivalent of the film in a camera. Blood vessels, the parts used for biometric identification, are found in the top layer of the retina and form a pattern that is unique to each individual.

Retina scan is one of the oldest biometrics. In the 1930s, research suggested that the blood vein patterns on the back of the eye were unique to the individual. The first commercially available identification systems were developed in the mid-1980s. Later developments made the scanner units smaller and less expensive; however, because of implementation costs, difficulty in collecting samples, and negative perceptions regarding intrusiveness, their use has declined significantly. High-security applications with low throughput requirements and relatively few authorized users is one of the few remaining uses of retina scan technology.

3.3.12 Voice Recognition

Voice recognition technology uses the unique aspects of human voice patterns to verify the identity of individuals. The fundamental theory for voice recognition is that every voice is distinct and unique enough to identify the speaker. The shape of the vocal tract changes as a person speaks. The different shapes that the vocal tract assumes and the individual's speaking behaviors contribute to the uniqueness of the voiceprint.

Currently, voice recognition is being used in a number of market sectors including warehouse and distribution, electronic commerce, financial services, government, healthcare, and telecommunications. Although not suitable for high-security solutions as a single method of access control, voice recognition technology is useful in lower security and in multimodal applications in combination with other biometrics and electronic access control technologies.

Some systems measure the rhythm, tone, and pitch an individual uses to repeat one or more passphrases. Newer systems use proprietary algorithms to analyze the vocal tract to generate a secure voiceprint. Another feature to increase the security of voiceprints is the use of random passphrases. A human can listen to and repeat a phrase that recordings cannot duplicate. Voice recognition technology continues to advance, and systems are becoming more sophisticated so that passphrases can consist of any phrase that the individual wishes to use in any language. The phrase itself is not important as long as it matches what the enrolled computer database expects. It is the unique characteristics of the voice itself that are patterned.

Voice recognition has only recently emerged as a means for physical access control. Voice recognition has been used in one form or another for almost 30 years, but it is only in the past few years that advances in computer processing power and software development have made it commercially viable. Prior uses were mainly for speech recognition purposes (i.e., translation of spoken words into text) or for logical access to computer systems.

3.3.12.1 Operation

Voice recognition can use any audio capture device. Most software contains extensive filters to distinguish between background noise and a user's spoken passphrase. In high noise environments, the system must use a noise-canceling, close-talk microphone that favors the user's voice and eliminates most of the extraneous surrounding noise. The ambient noise levels at the points of access and enrollment should influence the choice of input device.

Figure 3-24 depicts the operation of a voice recognition system. During enrollment, an individual repeats a passphrase or a sequence of numbers. Passphrases should be approximately 1 to 1.5 seconds in length. Very short passphrases lack enough identifying data, and long passphrases have too much data. Both cases result in reduced accuracy. The individual repeats the phrase a set number of times, and enrollment usually is completed in approximately 30 seconds, which is slightly longer than most other biometric access control systems require.

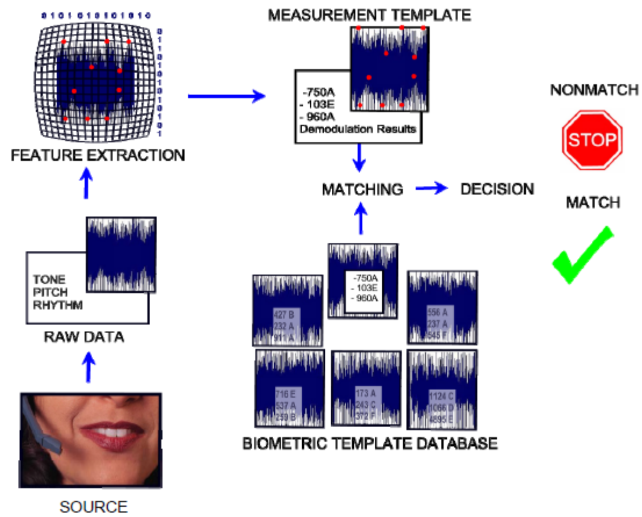


Figure 3-24. Voice Recognition

3.3.12.2 Applications

Applications of this technology include warehouse inventory control and shipping, banking, corrections facilities, general access control, securing access to confidential information, call centers, and access to voice portals.

3.3.12.3 Performance Metrics

The performance of voice recognition systems can vary with the quality of the audio signal and differences between enrollment/recognition devices and ambient environments. The same types of devices should be used for enrollment and recognition.

FMR and FNMR can be higher in this type of system compared to several other biometric technologies. Although these rates are scalable depending on the system application, the units may have either a high tolerance (low security) or high FNMRs.

The verification process in voice recognition can require from 2 seconds to 10 seconds, depending on the system. This rate will affect throughput.

The size of voice recognition templates can be a storage problem for large user populations.

3.3.12.4 Vulnerabilities

Concerns about the user having an illness that affects the quality of the spoken responses have been minimized through software development. Voiceprints are generated based on the vocal

tract and learned speaking habits. Common colds do not affect these traits; however, if the user contracts laryngitis, accuracy of the measurement would be diminished.

No individual can mimic the unique voice patterns of another person. Mimics depend on mannerism, rhythm, and intonation to impersonate an individual, but voice recognition technology focuses on different characteristics than does the human ear. Any attempt to breach a voice recognition system using an impersonation of an authentic enrolled user fails because the system relies on the unique tones produced by the vocal chords rather than the mannerisms and rhythms of speech.

Tape-recorded attacks on the access control system are also easily defeated. No recording device can perfectly reproduce the characteristics of the vocal tract, so recorded voices typically fail to match the template. Also, most new systems utilize real time random prompting for passphrases and the responses cannot be pre-recorded.

Since vocal tracts change with age, most current voice activated access control systems track gradual changes to a user’s voiceprint over time to compensate.

Issues that can affect voice recognition template quality include:

- Different enrollment and recognition capture devices
- Different enrollment and recognition environments
- Individuals speaking in a low voice or speaking softly
- Poor placement of the microphone or other capture device
- Phone line quality, where the passphrase is repeated into a telephone.

3.3.13 Signature Dynamics Recognition

Dynamic signature recognition is a biometric technology that is used to identify a user from a handwritten signature. This is done by analyzing the shape, speed, stroke, pen pressure, and timing information during the act of signing. Signature dynamics is not frequently used for physical access control.

Many people are aware of the concept of signature analysis, which consists of determining if a signature was probably written by the same person who wrote a reference signature. Signature dynamics, on the other hand, takes into account how the signature was made. The changes in speed, pressure, timing (i.e., natural rhythms), and sequential stroke patterns that occur when an individual signs his/her name are learned behaviors unique to that individual. While it is possible for a computer, a copy machine, or an expert forger to duplicate the look of a signature, the other components are unique to the original signer. Although slight variations in a person’s handwritten signature are common, the consistency that natural motion and practice create over time is a measurable, unique pattern.

Signature verification has a high user acceptance rate, because the signature is so often used for identification in other contexts. Legal documents, credit charges, and many other daily transactions use signatures for identification and processing.

3.3.13.1 Operation

Signature dynamics technology uses the distinctive aspects of the signature to verify the identity of the individual. The technology examines the behavioral components of the signature such as stroke order, speed, acceleration, and pen pressure to construct a multi-dimensional digital image of the signature (Figure 3-25).

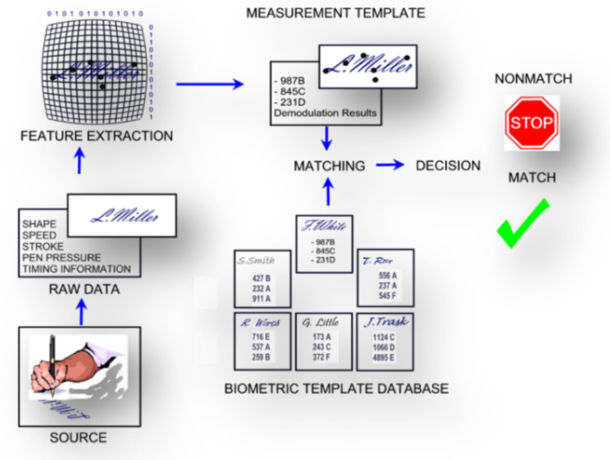


Figure 3-25. Signature Recognition

A signature is recorded on the screen of a digital tablet with a stylus. The surface of the tablet screen is pressure sensitive to record parameters. The stylus on some tablets has a pressure sensitive tip that records writing pressure in addition to the measurements from the screen. At least one manufacturer has developed a special motion sensitive pen that records the signature as it moves across a special writing surface.

During enrollment, the system develops a template based on the most common and notable characteristics of the user's signature style. The user provides several signatures that are similar enough that the system can locate a large percentage of the common characteristics among the signatures. Some systems generate a single reference template, while others record all the enrollment signatures to be reference templates. These reference templates are either saved in a central database or recorded on a smart card that the user carries. The location of the reference template depends on the system and the facility's overall security configuration.

The user must be relatively consistent during subsequent signature events for the system to verify identity. Most signature-based systems modify the reference template with each event to accommodate changes in personal style over time.

3.3.13.2 Applications

Signature dynamics access control systems can be used for either identification or verification. These systems are often implemented in controlled access situations where signature or written input processes are already in place. Examples include applications where written access logs are maintained, in financial institutions, or at prescription counters in pharmacies.

3.3.13.3 Performance Metrics

Enrollment times typically take up to 30 seconds from start to finish, because each user provides several signatures for the system to analyze.

Verification times vary from 4 to 6 seconds. Throughput rates are generally less than 10 users per minute in practice. The FMR is typically low, on the order of 0.001 percent. On the other hand, FNMR can be typically around 10 to 20 percent or higher if the user does not have a consistent signature which can be a major issue in most applications.

3.3.13.4 Vulnerabilities

There are unique vulnerabilities associated with signature dynamics:

- Signature dynamics access control requires a digitizing tablet, motion sensitive stylus, or other capture device that can become worn over time.
- Since most users are not accustomed to signing on a digital tablet, their signatures may differ from those placed with ink on paper. This increases the potential for false rejection.
- The user's signature must be consistent from event to event. Since the measured characteristics of the signature are not purely physical, the user's behavior can affect the ability of the system to verify identity more than most other biometric access control systems; however, this does not mean that an imposter can easily gain admittance.
- Signing in a different position (e.g., sitting versus standing) may cause the system to falsely reject an authorized user.
- Individuals with muscular illnesses and people who sign only with initials might have higher rejection rates.

3.3.14 Multimodal

Single biometric access control systems must often contend with noisy sensor data and unacceptable error rates. Multimodal biometric systems provide the ability to combine two or more complementary modes for verification and identification, as shown in Figure 3-26. The most obvious reason for using multimodal biometrics instead of a single modality is to make access control operations more secure. It seems logical that combining systems should make spoofing more difficult and should result in overall lower error rates. There are ways to combine the outputs from biometric systems to achieve this goal, which is a process called fusion.

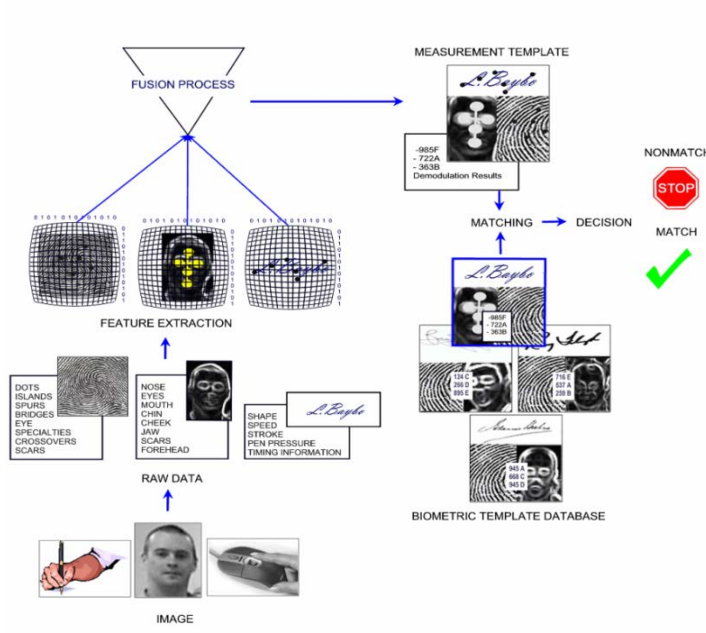


Figure 3-26. Multimodal Biometric System

The current challenge is to design a biometric access control system with as small an error rate as possible, that will cover the entire group of individual users, and that cannot be compromised under any reasonable scenario. True multimodality implies the ability to analyze several biometric traits simultaneously, instead of analyzing different biometric traits one at a time. One of the newest

technologies available combines multiple modalities, such as finger vein and fingerprint, and captures and processes the two sets of biometric data at the same time using a single device.

3.3.14.1 Operation

Middleware is a term used for a computer program that functions as a go between for two other programs. Fusion is typically performed in middleware using proprietary techniques that weigh the output from multiple biometric detection systems on a predetermined scale based on the access control system's use and facility's need. Some schemes can adjust the biometric detection signal weighting factors as a function of the individual user so that persons who cannot give a good sample for a particular biometric element can still use the system. Fusion schemes can operate at the feature extraction level (combining extracted features), at the confidence level (combining matching scores), and at the abstract level (combining accept/reject decisions).

In a multimodal scheme, multiple biometric systems send outputs to a single application that compares those outputs to a base reference. This comparison occurs at different levels within the overall system depending on the proprietary structure of the system which results in generating the signal to grant or deny access.

3.3.14.2 Applications

Multimodal biometric access control systems are most feasible for very high-security situations. These systems may use characteristics from the same biometric attributes or from different ones, but all samples are collected at the same time. For example, face, fingerprint, and iris may be captured and weights assigned to the match score of each modality for a higher confidence match/no match decision. Another example is finger vein combined with fingerprint recognition.

Consideration for selecting the modalities, sensors, and fusion approach must not only take facility security needs into account, but also convenience and the amount of user training required. User acceptance is paramount to system use. The best biometric system will become ineffective if it is difficult to use or easy to bypass using other means of access.

3.3.14.3 Performance Metrics

Operating performance metrics for multimodal systems are difficult to quantify since they depend on the single biometric systems selected and how they are combined. In general, a multimodal system should exhibit lower FMR and FNMR rates than any of its constituent parts would individually exhibit.

3.3.14.4 Vulnerabilities

The most serious vulnerability for multimodal systems relates to their complexity. The combination of different biometric subsystems can be confusing for the user unless the implementation schemes make sense from a human factors and operations standpoint. Systems that seem overly complex or restrictive for the anticipated level of security required should be closely scrutinized to ensure that facility requirements, as well as user needs, are being adequately addressed.

3.4 Assistive Technology

Assistive technology in access control incorporates products that allow people with physical or cognitive impairments to enter or exit a controlled area. This also includes the process of selecting, locating, and using these technologies. Assistive technology's use has improved engineering designs and well-planned user interfaces to help disabled individuals achieve previously unreachable goals. Often an assistive technology is simply an existing device or technology that has been modified to suit the abilities of a handicapped individual or group. While there is no single assistive technology that can meet the requirements for all disabilities, the operation of many existing access control systems can be improved with assistive technology and applications of universal design techniques, which strive for flexibility, intuitive operation, and tolerance of errors and faults. Disabled employees and other authorized facility users may be eligible to request reasonable accommodations under the ADA. Assistive technology is an important element of the design of any access control system.

This section will briefly examine each of the access control technologies already reviewed to identify potential changes and modifications that could improve accessibility for people with some types of impairment or disability.

3.4.1 Operation

Assistive technology can be installed in accordance with the ADA in newly constructed facilities, during some remodeling projects, and when required in special situations. Installing a voice recognition system during a remodeling project to augment a fingerprint access control system is an example of an assistive technology application for those who have lost limbs or have abraded fingertips. Access control assets, procedures, and the application of assistive technologies should be audited periodically, especially during facility safety reviews and inspections.

3.4.2 Applications

- Barriers: fixed and portable barriers can blend into the surroundings and become a safety hazard for people with visual impairments. Barriers should be painted in high contrast color schemes to enhance visibility. In some cases, it may be appropriate to add some type of audible proximity alarm.
- Obstacles: turnstiles, portals, and mantraps should be marked with sufficient contrast so they can be easily seen by visually impaired persons. The level of force used by powered equipment such as doors or turnstiles and the effort required to operate the equipment should be appropriate to the application. Facility managers should consider how persons with restricted mobility or strength limitations will move through the obstacles and provide alternatives when necessary.
- Bollards: fixed and portable bollards often are large, heavy, stationary objects that exhibit some aesthetic or architectural design that contributes to the safety and beauty of the surroundings. Bollards are most often used to restrict vehicle traffic, but allow pedestrian traffic to pass without restraint. Generally, the minimum space between the bollards should be no less than 4 feet, to allow access for a person walking beside another using a wheelchair.

- Guard Facilities: often people with limited hearing have difficulty communicating through Plexiglas or other safety barriers. A telephone or intercom is an example of an assistive technology that could be used in this situation.
- ID Cards and Badges: many agencies require that ID cards and badges must remain visible at all times. Several alternative attachment devices should be made available as required in certain situations. For example, a person using health support equipment might prefer a clip-on badge to a lanyard badge, to avoid the badge becoming entangled with the support equipment.
- Smart Cards and Devices: card readers and keypads or other input devices should be within reach of wheelchair-bound persons and those with mobility limitations. Signage may be required near the reader to explain its operation. Braille text or illustrated instructions may be necessary for those with sensory or cognitive disabilities. Auditory output, such as a chime or buzzer, can be used to inform persons with visual disabilities that the access control system has cycled. An intercom system at the access point can provide a link for further assistance when necessary.
- Magnetic Stripe and Keycard Door Systems: assistive considerations for these systems are similar to those enumerated for smart cards and devices.
- Key fobs: people with limited mobility often can use key fobs to unlock doors and grant access to visitors and delivery personnel. When fobs are used in this way, an intercom system at the access point improves the system's utility and security. Many fobs have a panic button that enhances the user's safety and security.
- Biometric Systems: biometric access control systems present various challenges when assistive technology solutions are required. For any such system, a small percentage of the population will be unable to enroll because of occupation, illness, or injury. When deploying a biometric access control system, it is essential to plan for alternative access control measures. For example, if authentication is usually performed using a fingerprint biometric system, there should be an alternative authentication system for those with amputations or abraded and/or callused fingers. An iris recognition system could be an alternative in this example.

3.4.3 Performance Metrics

The U.S. Access Board is an independent federal agency that promotes equality for people with disabilities through leadership in accessible design and the development of accessibility guidelines and standards. *ADA Accessibility Guidelines (ADAAG)* provides detailed guidance and specific standards for accessibility to buildings and facilities by individuals with disabilities under the ADA of 1990. The publication should be consulted by agencies seeking to implement assistive technologies.

3.4.4 Vulnerabilities

Generally, the changes made to accommodate people with disabilities benefit everyone. However, access managers should be careful that accommodations made for disabled people do not enable others to bypass or otherwise compromise the system.

4. VENDOR SELECTION GUIDELINES

Selecting an access control system vendor can be a challenge. Professional industry support is available from a host of companies, some of which offer a full suite of services and products. Others may offer more specialized services as designers, manufacturers, suppliers or authorized equipment dealers, installers, or integrators. The access control market evolves continuously with many vendors both entering and leaving the marketplace. Organizations may have internal experts that can fill certain roles, but any new, expanded, or upgraded access control system will require engagement with some form of professional industry support.

4.1 Selection Criteria

Experienced vendors may provide invaluable expertise to organizations seeking upgrades and integrations of older technology access control systems; however, some new vendors may have more specialized expertise in a particular emerging technology. Determining the most important criteria prior to selection is a fundamental step in finding the best suited vendor. Criteria can include the vendor's previous experience and past performance with access control products and services, their level of sophistication with design, installation, and integration of access control components, technical support offered, and total cost.

4.2 Vendor Resources

Selecting a well-qualified and experienced vendor with the capabilities to meet specific requirements will help increase the quality and performance of the overall access control system. The following organizations' websites provide information on access control system vendors, their related areas of expertise, and their contact information:

- ASIS International
- IEEE Xplore Digital Library
- Security Industry Association
- Security Magazine
- SANS Institute.

Appendix A. DEFINITIONS

Definitions of terminology commonly used and/or associated with access control technologies are provided below.

Access card–A coded card, which is presented to the access control system/card reader to gain access to facilities. It can also be used as a photo ID for the card holder.

Access point–The entry and exit point of a protected area.

Annunciator–An audio or visual alarm that indicates which alarm point has been activated.

Anti-passback–A feature of the access control system that prevents an individual from passing back their card or badge to attempt to gain access for an unauthorized person. The system shows the individual as in or out. Once in, the system will not allow the same card to enter again, and once out, the system will not allow the same card to exit again.

Authorized person–An individual who has been granted access to a secure space.

Badge–A physical token issued by an access control authority to show authorization.

Barcode–A form of coding using vertical bars of varying thickness and height.

Barcode reader–A device designed to read a barcode.

Biometrics–The ability to use the physical and behavioral characteristics of an individual for identification or verification purposes.

Card reader–A device used to interpret access card data.

Closed-circuit television (CCTV)–A video surveillance system using video cameras to transmit images to a specific location and set of monitors.

Controller–A specialized electronic device that manages access for a facility. May also be called panel or control panel.

Electronic access control–Controls access to a physical space through the use of electronic components including locks, readers, sensors, or buttons.

Enrollment–Assigns an identity in the access control system.

Equal error rate (EER)–The point on a graph, where the false match rate (FMR) and false non-match rate (FNMR) intersect for a given access control system. The smaller the EER, the more accurate the access control system.

Fail-safe–The ability of a system to automatically unlock access control points, allowing for emergency egress upon loss of power.

Fail secure–The ability of a system to automatically lock access points to prevent unauthorized access upon loss of power.

Failure to enroll (FTE)–The probability that a user will be unable to enroll in a biometric system due to insufficiently distinctive biometric samples.

False acceptance rate (FAR)–The probability that an access control system will confuse two individuals and grant access to an unauthorized individual. This is also called a false match rate (FMR).

False match rate (FMR)–The probability that an access control system will confuse two individuals and grant access to an unauthorized individual. This is also called a false acceptance rate (FAR).

False non-match rate (FNMR)–The probability that an authorized individual's data will not be matched to corresponding data in the access control system database. This is also called a false rejection rate (FRR).

False rejection rate (FRR)–The probability that an authorized individual's data will not be matched to corresponding data in the access control system database. This is also called a false non-match rate (FNMR).

Finger pattern area–The area of the finger that features the loops, whirls, and arches used in fingerprint recognition.

Fingerprint minutiae–The discontinuities that interrupt the smooth flow of fingerprint ridges and the abrupt ridge endings.

Fingerprint sensor–A biometric sensor that reads a fingerprint.

Hand geometry–An access control technology which uses variations in hand and finger size and shape to verify identity.

Identification–The act of recognizing an individual as unique from all others.

Key fob–A small proximity transmitter that can interface with an access control system.

Keyless access control–An entry control system using a means other than a key, such as a digital keypad.

Keypad–An input device for an access control system.

Magnetic keycard–A card containing thousands of magnetic bits or particles that can be arranged in an approved pattern to allow access.

Magnetic stripe–A band of ferrous material that is sealed in or onto a card and stores data.

Mantrap–An arrangement of doors, usually forming a small corridor or booth, which allows a person to enter and be identified before proceeding into a controlled area.

Middleware–A general term for any software that tends to mediate between two other software programs. For example, an access control system and a computer operating system use middleware to communicate with each other.

Mixed technology sensor–A detector that uses two or more sensing technologies to reduce false alarms.

Multimodal–The ability to combine multiple types of access control technology in the same session.

Operations center–A station within the facility where personnel monitor, assess, and respond to alarms and/or trouble signals. May also be referred to as a Control Center.

Performance metrics–Characteristics of access control systems that are used to evaluate system performance.

Personal identification number (PIN)–A unique set of digits that are used as a password for an access control system.

Portal control–An ingress/egress system using two doors where one door is locked at any given time. This varies from mantrap which locks both doors.

Proximity card–A radio frequency based access control technology that utilizes a micro electronic circuit. The micro electronic circuit is activated when the card is presented to a proximity card reader. Once activated, the information stored on the card can be transmitted and used to grant or deny access.

Reader–Any device that reads encoded information from a card or token and transmits information to a control panel or access control device.

Smart card–An identification card containing an integrated circuit allowing it to receive and store data, which can then be read by an access control system.

Stand-alone–An access control device that independently operates without communicating with a central controller.

Tailgating–The act of an unauthorized person attempting to gain access to a controlled space by following closely behind an authorized person. This is also referred to as piggybacking.

Threshold adjustment–A change made to a biometric system's processing algorithms that changes the performance metrics.

Throughput–The number of people passing through a system over a given period of time.

Turnstile–An access control point utilizing a gateway, usually a rotating or recessing barrier.

Underwriters Laboratories (UL) labeled–Signifies that production samples of the product have been found to comply with established UL requirements and standards.

Verification–The act of verifying an individual's identity.

Wiegand card–An access card that has two rows of embedded specially treated ferromagnetic wires that can be read by a device.